FOR THE COMMON DEFENSE OF CYBERSPACE: IMPLICATIONS OF A US CYBER MILITIA ON DEPARTMENT OF DEFENSE CYBER OPERATIONS

A thesis presented to the Faculty of the US Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

PAUL W. TINKER, MAJOR, US AIR FORCE
B.S.E.E., Western New England University, Springfield, Massachusetts, 2003
M.S.E, University of Wisconsin-Platteville, Platteville, Wisconsin, 2010

Fort Leavenworth, Kansas
2015

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-06-2015	Master's Thesis	AUG 2014 – JUNE 2015

4. TITLE AND SUBTITLE

For the Common Defense of Cyberspace: Implications of a US Cyber Militia on Department of Defense Cyber Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Paul W. Tinker

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

US Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This work examines the current cyber space threat against the US, the current gaps in combating it, and how a US cyber militia might fill those gaps. Militias have historically been used by the US as an emergency measure to protect national security and to defend the homeland in lieu of a regular standing force. Currently, there are cyber militias being utilized worldwide to do just that, but along virtual borders vice land, sea, air and space. Countries such as Estonia and India have combated State and Non-State actors successfully with all-volunteer cyber militias performing an array of tasks in the common defense of their cyber domain. The research compares the organizational structure, mission, formative strategic context, and noteable actions of six volunteer cyber organizations through a qualitative case study analysis. Coupled with an extensive literature review, this study examines possible implications of a US cyber militia on US cyberspace security. The focus of the conclusions and recommendations are on the short and long term impacts a cyber militia could have on US defense operations.

15. SUBJECT TERMS

Cyber Militia, Cyberspace, Cyber Operations, Joint, Cyber Command

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	113	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Paul W. Tinker

Thesis Title: For the Common Defense of Cyberspace: Implications of a US Cyber Militia on Department of Defense Cyber Operations

Approved by:

_____, Thesis Committee Chair
Herbert Merrick, M.S.

_____, Member
LTC Andrew K. Murray, MPA

_____, Member
Tony R. Mullis, Ph.D.

Accepted this 12th day of June 2015 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

FOR THE COMMON DEFENSE OF CYBERSPACE: IMPLICATIONS OF A US CYBER MILITIA ON DEPARTMENT OF DEFENSE CYBER OPERATIONS, Major Paul W. Tinker, 113 pages.

This work examines the current cyber space threat against the US, the current gaps in combating it, and how a US cyber militia might fill those gaps. Militias have historically been used by the US as an emergency measure to protect national security and to defend the homeland in lieu of a regular standing force. Currently, there are cyber militias being utilized worldwide to do just that, but along virtual borders vice land, sea, air and space. Countries such as Estonia and India have combated State and Non-State actors successfully with all-volunteer cyber militias performing an array of tasks in the common defense of their cyber domain. The research compares the organizational structure, mission, formative strategic context, and noteable actions of six volunteer cyber organizations through a qualitative case study analysis. Coupled with an extensive literature review, this study examines possible implications of a US cyber militia on US cyberspace security. The focus of the conclusions and recommendations are on the short and long term impacts a cyber militia could have on US defense operations.

ACKNOWLEDGMENTS

I wish to acknowledge the members of my committee for their direction and assistance provided in writing this thesis. Without their diligent efforts, this work would not have been possible. I would especially like to thank my chair, Mr. Herb Merrick for keeping me on track, organizing committee meetings, scheduling the oral comprehensive board and of course the thesis defense. I also wish to thank him for the many hours of mentoring throughout the year as my staff faculty advisor.

Additionally, I would like to recognize my subject matter expert Lieutenant Colonel Andrew Murray for ensuring the issues were discussed in depth while also serving as the necessary sounding board on which theories to pursue or not. I also wish to recognize Dr. Tony Mullis, who was critical in safeguarding the high standards of the Command and General Staff College's scholastic rigor and provided the contextual breadth for the topics explored for this research. Finally, I would like to thank my roommate, Major Andy Walsh, who provided timely moral support and provided valuable insight into the mind of a cyber security professional.

Electrical Engineers are not typically known for their ability to organize words into the coherent thoughts required to articulate months of research and so I am extremely grateful to all of these gentlemen for the patience they exhibited in guiding me through this process. Researching a topic and writing a thesis has been a lifelong goal and it would not have happened without their help.

TABLE OF CONTENTS

ACRONYMS

CDL	Cyber Defense League
CERT	Computer Emergency Readiness Team
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DoD	Department of Defense
DoJ	Department of Justice
DSB	Defense Science Board
EFF	Electronic Frontier Foundation
FY	Fiscal Year
ICA	Indian Cyber Army
LOAC	Law of Armed Conflict
NCA	National Command Authority
NDAA	National Defense Authorization Act
NSA	National Security Administration
NSS	National Security Strategy
SANS	System Administration, Audit, Networking, Security
UK	United Kingdom
UN	United Nations
US	United States
WARP	Warning, Advice, and Reporting Point

LIST OF FIGURES

Page

TABLES

Page

CHAPTER 1

INTRODUCTION AND OVERVIEW

> There should be [no] doubt in anybody's mind that the cyber challenges we're talking about are not theoretical. This is something real that is impacting our nation and those of our allies and friends every day.[1]
>
> — Admiral Michael S. Rogers, 2014

> The Congress shall have power…to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions.
>
> — *US Constitution, Article 1, Section 8, Line 15*

Since their inception, the executive and legislative branches of the United States (US) have worked in concert to fend off various threats for the common defense of the country.[2] The US is now facing perhaps one of the most complicated, persistent and technical threats in its history via the man-made domain known as Cyberspace. This threat is complex because it is constantly evolving, lacks attribution, is easily accessible, relatively cheap, and it is growing exponentially. As this threat develops, the resources required to defend against it have and will continue to grow unless the government can create more innovative defenses.[3] Specifically, the amount of time, money, and personnel required to combat the escalating threats in cyberspace have increased exponentially in

---

[1] Cheryl Pellerin, "Cyber Chief Details Cyber Threats," DoD News.com, accessed 9 February 2014, http://science.dodlive.mil/2014/12/02/cybercom-chief-details-u-s-cyber-threats.

[2] Alan Millett, Peter Maslowski, and William B. Feis, *For the Common Defense: A Military History of the United States from 1607 to 2012*, 3rd ed. (New York: Free Press, 2012).

[3] Sean Heritage, "Creating a Wake" (Lecture, Army Cyber Institute Cyber Talks Address from Fort McNair, VA, 15 March 2015).

order for the US to keep its long held advantages in the other warfare domains. This dramatic investment by the US has seemingly kept pace with the threat, and currently shows no signs of slowing down.

Exacerbating the issue is the National Command Authority's (NCA) Cold War spending propensity of continuously throwing money into expensive technologies instead of looking for innovative ways to protect its cyber domain. This tendency has constrained decision makers by forcing the application of current organizational structures, doctrine, equipment and training methods designed for use in the physical domains of land, sea, air, and space. For example, the Department of Homeland Security's (DHS) network intrusion system known as Einstein 3 is expected to exceed 2 billion in procurement dollars[4] and additionally, the annual operating expenses of the DoD's Cyber Command is now more than 70 million dollars.[5] The US government is spending an average of 13 billion dollars a year over the last five years and the US private sector has averaged just under 20 billion. Comparatively, in 2014, all of Western Europe spent a combined 16 billion and the entire Asia-Pacific region spent 14 billion.[6] Simply put, no other country in the world spends more money on cyber security than the United States. Those who

[4] Ellen Nakashima, "Cybersecurity Plan to Involve NSA, Telecoms," *Washington Post*, 2 July 2009, accessed 19 April 2015, http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771_pf.html.

[5] White House, *President's Budget Request 2015* (Washington, DC: White House, 2015), 26.

[6] Newly Purnell, "Cyberdefense Spending Rises Amid High-Profile Hacks," *Wall Street Journal*, accessed 19 April 2015, http://www.wsj.com/articles/cyberdefense-spending-rises-amid-high-profile-hacks-1428487519.

argue that the US spends more because it is attacked more do not fully appreciate the true nature of cyber warfare: an asymmetric and a hybrid breed of conflict fought by both State and Non-State actors alike using all available means to oppose one's will.[7] The type of thinking that has driven increased government spending has limited the innovation required to address this complex problem properly, especially so in an environment where there is a dearth of the most important resource in fighting this threat: subject matter experts. With an estimated 700,000 additional cyber security experts needed nationwide by 2018,[8] US Navy Captain Sean Heritage, executive assistant to Admiral Michael Rogers, summed up the cyberspace challenge very succinctly by stating, "Cyber is all about expertise."[9] Yet, the military eliminates 70 percent of eligible cybersecurity experts because of its entry requirements such as height, weight, education, and appearance.[10] Major General Allen Batschelet, commanding general for the US Army Recruiting Command has bemoaned this fact. He concluded, "There's a reliance on an ever-smaller group of people to serve and defend the country."[11]

---

[7] Susan W. Brenner and Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts.: an Article From: Vanderbilt Journal of Transnational Law* (Nashville, TN: Vanderbilt University, School of Law, 2010), 4.

[8] Department of Defense, *Cyber Operations Personnel Report* (Arlington, VA: Department of Defense, 2011), 5-7.

[9] Heritage.

[10] Clifford Davis, "Army Says Only 30% of Americans Could Join," *The Florida Times-Union*, 24 October 2014, accessed 2 April 2015, http://www.military.com/daily-news/2014/10/24/army-says-only-30-percent-of-americans-could-join.html.

[11] Ibid.

For its part, the current US Government administration has prioritized cyber security higher than other previous administrations. It has increased cyber security spending every year except once since 2008, more than doubling the amount from 6.7 billion dollars in Fiscal Year 2008 (FY08)[12] to a proposed 14 billion dollars proposed for FY16.[13] Additionally, the administration has worked to grasp the cyberspace issues better through numerous agency audits, congressional hearings, and science board studies. It continues to push for assured access to the cyber domain in its most recent *National Security Strategy*.[14] This commitment of organizational resources and the now billions of dollars pumped into boosting US cyber security capabilities has proven just how serious the US Government believes cyber superiority is to securing its vital interests. Specifically, the 5.5 billion dollars allocated to the Department of Defense (DoD) for FY16 cyber technology procurements represents its third largest modernization program expenditure for the up-coming year. Only the Navy's new vessel procurement of $9

[12] Greg Otto, "4 Charts That Will Keep Federal CIOs Up at Night," *Fedscoop*, 23 January 2015, accessed 27 March 2015, http://fedscoop.com/4-charts-that-will-keep-federal-cios-up-at-night.

[13] Andrea Shalal and Alina Selyukh, "Obama Seeks $14 Billion to Improve Cyber Defense," *Reuters*, 2 February 2015, accessed 27 March 2015, http://www.huffington post.com/2015/02/02/obama-cybersecurity-defenses_n_6595620.html.

[14] White House, *National Security Strategy* (Washington, DC: White House, March 2015), 15.

billion and the Air Force's $11 billion for 57 Joint Strike Fighters represents a larger defense investment.[15]

However, the DoD needs to do more. Based on several reports to include the Defense Science Board's 2013 report on *Resilient Military Systems and the Advanced Cyber Threat,* there is an argument that simply throwing more and more resources at the problem may not be the best course of action. The 2014 National Defense Appropriations Act (NDAA) directed the DoD to investigate and assess among other things, its current cyber operations structure.[16] Additionally, the 2014 NDAA directed the Secretary of Defense to conduct an analysis of current cyber operations to include the concept of employment of cyber forces.[17] In response, the DoD released a report citing progress amongst the services but concluded that, "additional capability may be needed for both surge capacity for the [active component forces] and to provide unique and specialized capabilities that can contribute to a "Whole-of-Government" and "Whole-of-Nation" approach to securing US cyberspace."[18] The report's focus was primarily assessing the current contributions of reserve component forces and whether or not their utilization

[15] Office of the Secretary of Defense, Comptroller, "FY16 Presidential Budget" (Briefing), Slide 8, accessed 15 February 2015, http://www.defense.gov/pubs/FY16 _Budge t_ Request_Rollout_Final_2-2-15.pdf.

[16] US Congress, Senate, Department of Defense Appropriations Acts, S. Res. 1590, 113th Cong., 1st sess. (July 13, 2013): 746.

[17] Ibid., 748.

[18] Department of Defense, *Cyber Mission Analysis* (Arlington, VA: Department of Defense, August 2014), 28.

could be directed in the cyber fight in other manners. Several additional findings from this report are discussed in the final chapters of this paper.

The NDAA directives and subsequent response by the DoD are a sign that there is a recognition amongst decision makers that the escalating costs of cyber security must be addressed in possibly unique ways. This paper argues that one such unique approach is one the nation has relied upon since its creation. Summon its citizens, with the desire and the requisite skillset required for the common defense of US cyberspace.

Issues

Assured access to the world's shared spaces has been a pillar of US national security strategy since 1782 through its "free ship, free space" policy concerning navigation of the seas.[19] The US has followed a similar policy in terms of assured access to cyberspace but there are unique and numerous issues that policymakers must understand to achieve this end state. These issues include competing funding priorities, a shortage in cyber security personnel, and a legislative system designed for rigor and not necessarily speed. However, the greatest issue is the nature of the threat itself. It is complex, uncertain, growing and affects anyone using a network. Public and private entities share varying degrees of vulnerabilities and the DoD is no different. There is an ever-increasing demand for weapon systems reliant upon cyber connectivity,[20] a growing

[19] Llewellyn Atherley-Jones, *Commerce in War* (Los Angeles, CA: Methuen and Co, 1907).

[20] Steven Tomanelli, *Federal Acquisition Regulation Desk Reference, 15-1* (Arlington, VA: LegalWorks, 2014).

number of provocateurs with access to powerful viruses, and the fact remains that despite the increase in the complexity of defensive measures, there has not been a corresponding decrease in cyber-attacks.[21] Additionally, current efforts to deter or coerce belligerents from performing cyber-attacks through political or economic sanctions will continue to remain ineffective until the anonymity provided by mostly open systems architecture is solved.[22]

No other domain is increasing its surface area faster as each new connected device provides at least one if not more possible ports of entry for exploitation.[23] These cyberspace vulnerabilities reside not only in the cyber domain but also in the physical domains of land, sea, air and space. The much-publicized cyber-attacks against Sony Entertainment Pictures and the corresponding threats against freedom of speech cemented in the imaginative collective just how potential adversaries can exploit the cyber domain. The convenience of connectedness is an attractive target due to its low risk, high reward calculus. What is less known, is that the DoD is confronted daily with over 10 million cyber related "attacks."[24] Per DoD doctrine, computer network attacks (CNA) or "cyber-attacks" are non-lethal yet intrusive cyber operations that are employed to manipulate,

---

[21] Defense Science Board, *Resilient Cyber Systems and the Advanced Cyber Threats* (Washington, DC: Department of Defense, January 2013), 26.

[22] Ibid., 30.

[23] Paul Rosenzweig, *Cyber Warfare* (Santa Barbara, CA: Praeger, 2013).

[24] Zachary Fryor-Briggs, "US Goes on Cyber Offensive," *Defense News*, 24 March 2014, accessed 2 November 2014, http://www.defensenews.com/article/20120324/DEFREG02/30324000, 1.

disrupt, or delete data on the DoD's vast inventory of net-centric command and control, automated information and weapon systems.[25] This number is quite astonishing and encompasses attacks via the internet, communication links, electronic warfare, and software designed to control hardware. It is important to remember that belligerent actors target anything they can in the electromagnetic spectrum. Justification for these actions varies from actor to actor but in general, the goal is to glean information or to possibly disrupt and even control these systems. As one former hacker admitted, "I loved hacking airwaves the most…everything that [lived] in the sky. Computer wireless networks are such a small part of the spectrum."[26] Even more disturbing is the fact that a threat may not even be a person sitting behind a computer screen. Automated systems known as "bots" will introduce malicious code to conduct "brute force" Distributed Denial of Service (DDoS) attacks faster than any group of humans. Malware, worms, and zero day exploitations routinely propagate through the endless recesses of the Internet, available to anyone with some money and a little skill.[27] Viruses can spread at alarming speeds and once it is through the hundreds of thousands of lines of code put in place to defend

[25] Chairman, Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: CreateSpace Independent Publishing Platform, 5 February 2013).

[26] Robert A. Grimes, "In his own words: Confessions of a Cyber Warrior," Infoworld.com, 9 July 2013, accessed 2 April 2015, http://www.infoworld.com/article/2611471/security/in-his-own-words--confessions-of-a-cyber-warrior.html.

[27] Warwick Ashford, "Powerful Cyber-Attack Tools Widely Available," *Computer Weekly*, 3 September 2012, accessed 2 April 2015, http://www.computerweekly.com/news/2240162578/Powerful-cyber-attack-tools-widely-available-say-researchers.

against it, there is a limited amount of options available to a victim to stop the attack let alone reverse the damage already done. Regardless of the type, cyber experts project attacks to increase in quantity, complexity and in ways not previously envisioned.[28]

After one understands the nature of the threat, the remaining issues deal with how to combat it. The first of which concerns the people that will create the necessary technology processes and systems used to combat complex cyber problems. Unfortunately, there are simply not enough cyber security professionals within the US enterprise, let alone the DoD to combat this threat.[29] Cyber Command's grand design is filling 6,000 cyber security slots by 2016. However, as of the end of 2014 they had only hired 2,400.[30] The Air Force has 11,000 cyber professionals (civilian, military and contractors) with the hopes of hiring at least 1,000 more by the end of FY16 (albeit only 200 additions have been currently authorized).[31] The US Navy's 10th Fleet wants 1,000

[28] Brett Williams, "Cyberspace: What is it, Where is it and Who Cares?" *Armed Forces Journal* (March 2014), accessed 25 March 2015, http://www.armedforces journal.com/cyberspace-what-is-it-where-is-it-and-who-cares.

[29] Francesca Spidalieri and Sean Kern, *Professionalizing Cybersecurity: A Path to Universal Standards and Status* (Newport, RI: Salve Regina Pell Center, August 2014).

[30] Michael Rogers, *Cybersecurity Threats: The Way Forward, Testimony Before House Intelligence Committee*, 20 November 2014.

[31] Stephen Losey, "Budget to Add 4,000 More Jobs," *Air Force Times*, 2 February 2015, accessed 8 April 2015, http://www.airforcetimes.com/story/military/careers/air-force/2015/02/02/budget-would-add-4000-active-duty-airmen-in-2016/22740199.

more "cyber sailors,"[32] and the Army, currently sitting at 1,000, wants to be at 5,000.[33] These personnel requirements have been driven by accessing the various mission components of a cyber organization (mission planning, coordinating, integrating, synchronizing, directing, conducting network operations), the scope of their cyberspace area of operations and the anticipated threat. Additionally, services are not just competing against each other for qualified personnel; they are competing against other US Government departments, agencies, and of course, private sector companies. A 2011 DoD report on cyber personnel outlined the need for not just additional expertise but the retention programs required to keep those already employed by the DoD.[34]

Simple math highlights an enormous personnel gap and Alan Paller, director of the SANS Institute, does not see that gap closing very quickly. "Right now, there aren't any people in the pipeline to fill those slots, there is no supply of them. If you hire someone, you are going to take them away from another company." Or perhaps another Government agency will hire them. DHS, the Department of Justice (DoJ), the Department of State (DoS) and the National Aeronautics and Space Administration

[32] Joshua Stewart, "Navy Wants 1,000 More Cyber Warriors," *Navy Times*, 23 April 2013, accessed 22 January 2015, http://archive.navytimes.com/article/20130423/NEWS/304230016/Navy-wants-1-000-more-cyber-warriors.

[33] Edward Cardon, "Army Cyber Capabilities" (Lecture, Advanced Operations Course Address to Command and General Staff College, Fort Leavenworth, KS, 3 December 2014).

[34] Department of Defense, *Cyber Operations Personnel Report* (Arlington, VA: Department of Defense, August 2011).

(NASA) are all currently looking to increase their pool of cyber security professionals.[35] Complicating this manpower problem is the estimate of 2,000 hours that Paller and other experts determined it would take of on-the-job training to bring a college graduate to the level necessary to defend a network from attack.[36] This number (approximately one year's worth of work or a "man-year") comes from the DHS "Cyberskills Task Force" report led by the SANS Institute and is an aggregate of estimates provided by various public/private companies involved with the study. These organizations included Time Warner Cable, Facebook, Sony, Northrup Grumman and the National Security Agency.[37] Finally, once a cyber security professional is trained, many argue, to include the head of Army's Cyber Command, Lieutenant General Edward Cardon, that it takes approximately five years to develop an effective cyber security professional.[38] The totality of the enterprise demand for personnel numbers coupled with the statements from Paller and General Cardon make a compelling case that the US is in dire need of a new pool of talent.

---

[35] This information was gathered through the DoJ, DoS, NASA, DHS, and USAjobs web pages.

[36] Robery Lemos, "Pentagon Recruiting Drive Targets Fivefold Increase in Cyber Command," *Eweek*, 30 January 2013, accessed 10 February 2015, http://www.eweek.com/security/pentagon-recruiting-drive-targets-fivefold-increase-in-cyber-command#sthash.HEqQH63L.dpuf.

[37] Department of Homeland Security, *Task Force on Cyberskills Report* (Washington, DC: Department of Homeland Security, 2012), 38-41.

[38] Cardon.

The next glaring issue is the enormous costs involved with cyber security and network defense. As stated previously, the US Government has earmarked almost 14 billion dollars for cyber security in FY16 and has invested almost 60 billion dollars over the past five years. The private sector spent a reported 250 dollars million spent last year.[39] There is an expected 14.6 percent increase this year, which is a faster growth rate than the government for the first time ever.[40] What is worrisome is that despite the increased expenditures from the cyber security enterprise the cost of attacking a network has remained relatively steady. This is due to the simple fact that the lines of code required to exploit a vulnerability has remained consistently small in comparison to the now intricate defensive systems produced to combat them.[41]

Finally, the legal issues can be described at best as, "complicated," and this study will not attempt to analyze these issues other than to provide high-level context to support the assumption that it will take several years to get correct. At its core, the legal issues in cyberspace concerning cyber warfare revolve around the varying interpretations of the *Jus ad Bellum* (right to war) and *Jus in Bello* (law of war) justification criteria. These criteria are consulted before engaging in war, in order to determine whether entering into

---

[39] US Department of Treasury, "Remarks of Secretary Jacob J. Lew at the 2014 Delivering Alpha Conference Hosted by CNBC and Institutional Investor," 14 June 2014, accessed 16 April 2015, http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx.

[40] Farrah Kim, "Private Sector Spending Accelerating," Telecom Reseller.com, 2 February 2015, accessed 1 April 2015, http://telecomreseller.com/2015/02/28/tia-cybersecurity-report-private-sector-spending-accelerates-after-years-of-underinvestment.

[41] Department of Defense, *Resilient Cyber Systems*, 26.

war is permissible. Additionally, *Jus in Bello*, refers to the aspect of public international law concerning acceptable justifications to engage in war and the limits to acceptable wartime conduct.[42] The effort to define and govern the conduct of individuals, nations, and other groups in war dates from antiquity. The crux of the legal issues stem from the simple fact that the United Nations (UN) Charter was written well before the Internet was created. The charter was written just after WWII to encompass kinetic, i.e. physical attacks and not cyber-attacks. Thus, the charter along with the Law of Armed Conflict (LOAC) do not currently apply and therefore a country would not be committing an illegal act by launching cyber-attacks against government-owned or civilian-owned targets.[43] Specifically, article 2 of the charter prohibits use of force by one state against another and there is as of yet, no definition of what a use of force is in cyberspace since cyber-attacks rarely cause physical damage. Attempts have been made to get the international community to follow the same set of rules but it has been slow going and there is little impetus for nations to define these rules that allow them to operate in "the gray."[44]

[42] Corrie Becker, "The Tallin Manual: The Legal Aspects of Cyber Warfare," Cyber Security and Research Institute, 15 October 2013, accessed 20 April 2015, http://www.cspri.seas.gwu.edu/blog/2014/7/25/the-tallinn-manual-legal-aspects-of-cyber-warfare.

[43] Brenner and Clark, *Civilians in Cyberwarfare: Conscripts*, 22.

[44] Becker, "Tallin Manual: Legal Aspects of Cyber Warfare."

Problem Statement

Cyberspace is a dynamic and complex environment filled with state and non-state actors exploiting vulnerabilities to garner political and economic advantages. To combat these actors, expertise, money, and a legitimate set of laws are required, none of which are easy to come by. Currently, there is a growing competition for cyber security professionals within the cyberspace enterprise. In addition, costs are increasing and both US and international cyber domain laws need to be addressed. For the DoD, the most glaring of these issues deals with manpower and its continued self-imposed limitations on who it hires. Thus, solving the cyber threat problem within the DoD is contingent on obtaining (and retaining) cyber security experts. This paper briefly explores these issues and suggests a possible solution in the form of a cyber militia.

Purpose and Significance of Research

To address the issues described above, the purpose of this research is to lay the groundwork for a better understanding of a volunteer organization and a framework that might provide better value in combating foes in cyberspace. The study will address the findings in the 2014 NDAA directed cyber security assessment report by discussing the possibility of a US cyber militia. This research will delve into what a cyber militia might look like; its roles, capabilities, limitations and most importantly the implications of what a cyber militia might have on current or future DoD cyberspace operations. The significance of the research performed is that by comparing and consolidating the advantages and disadvantages of several current cyber militias, a better understanding of their capabilities can be ascertained. Additionally, by exploring the topic of a US cyber

militia, initial social, political and operational implications can be framed for future researchers and decision makers to address.

Research Question

The central question this thesis addresses is: Could a US cyber militia as constructed in this study be a practical organizational augmentation in support of DoD cyber operations? To answer this the following secondary questions were considered:

1. What is the current threat to the DoD in the cyber domain?
2. How has the United States historically used militias?
3. What is a cyber militia, where are they currently located?
4. How and why are cyber militias currently employed?
5. Could the DoD incorporate a cyber militia as currently organized?
6. How could the US best employ a cyber militia?

Assumptions

This paper assumes that there is a correlation between organizational structure, expert personnel, and success in cyber warfare. This paper also assumes that various technologies will not be fully implemented in the next three to five years. Internet Protocol Version 6 (IPV6), Public Key Infrastructure, and "hack proof" code are all viable options currently being pursued to mitigate cyber threats but will not be available or implemented in the near future. Additionally, this research assumes that the internet will not change its architecture significantly enough to decrease its inherent security vulnerabilities. Finally, for the purposes of this study it is assumed that the majority of the issues requiring legal attention will be addressed to meet the 2015 NSS policy

directive within the next two to three years within the US and next five to seven years internationally.

Definition of Terms

The Committee on National Security Systems (CNSS) is a United States intergovernmental organization that sets policy for the security of US information security systems. CNSS Instruction 4009 is a glossary of terms related to cyberspace activities and was the primary reference for the definition of terms used in this thesis. Other definitions were taken from Chairman, Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, JP *1-02, Terms and Definitions* or as otherwise noted.

Bot: A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote command and control of a remote administrator.

Cyber-attack: Non-lethal offensive operation intended to create physical effects or manipulate, disrupt, or delete data.

Cyber Incident: An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Cyber Militia: A collection of volunteers organized in some manner to perform operations in or pertaining to cyberspace.

Cyberspace (Cyber Domain): Cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an

Internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them.

Cyberspace Operations: The employment of cyberspace capabilities where the primary purpose is to achieve objectives (goals) in or through cyberspace.

Defensive Cyber Operations: Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

Distributed Denial of Service (DDoS): A denial of service technique that uses numerous systems to perform an attack simultaneously.

Hacker: An unauthorized user who attempts to or gains access to an information system.

Hacktivist or hacktivism (a portmanteau of hack and activism): Is the subversive use of computers and computer networks to promote a political agenda. With roots in hacker culture and hacker ethics, its ends are often related to the free speech, human rights, or freedom of information.[45]

Malware: Software that compromises the operation of a system by performing an unauthorized function or process.

Offensive Cyber Operations: Cyberspace operations intended to project power by the application of force in or through cyberspace.

---

[45] Peter Krapp, "Terror and Play, or What was Hacktivism?" *Grey Room MIT Press* (Fall 2005), accessed 4 April 2015, http://www.academia.edu/307639/Terror_and_Play_or_What_Was_Hacktivism.

Open Architecture: An architecture whose specifications are public. This includes officially approved standards as well as privately designed architectures whose specifications are made public by the designers. The opposite of open is closed or proprietary.[46]

Response Action: Defensive cyberspace actions taken to defend the network which occur outside of the DoDIN.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Limitations

The primary limitations of this study were the time allotted to complete it and the seemingly endless amount of cyberspace related material published on a weekly basis. With new journal articles, reports, speeches, and even US Presidential Executive Orders produced during the research period, it became an almost daily chore to assess the statements made throughout this paper and determine if they were still viable. An additional limitation was the willingness of current cyber operators to discuss the topic. Though there was interest, most were not willing to go on the record to elaborate on their thoughts. Overcoming these limitations can be accomplished through the additional research proposed in chapter 5.

[46] Webopedia, "Open Architecture," accessed 13 April 2015, http://www.webopedia.com/TERM/O/open_architecture.html.

Delimitations and Scope

The author recognizes that cyber warfare has many forms and that the Internet is just one avenue for potential attackers. However, the majority of the research conducted for this study was focused on the defense of cyberspace via the Internet as it continues to be the tool of choice by a preponderance of attackers due to its open architecture and the anonymity it provides. Other attack avenues are discussed briefly, such as social engineering and poor communications security practices but only in relation to how a cyber militia might be able to hone organizational preventative measures to address those threats. Additionally, the research focused on what the DoD could do organizationally to better defend against the threat, keeping in mind that there is a need for constant interagency coordination between all US Government departments to include DHS and DoJ. Finally, discussions will expand primarily upon defensive operations due to the lack of unclassified information on DoD offensive operations, but that does not necessarily limit any conclusions that might suggest cyber militias might best be employed in an offensive manner.

Summary and Conclusions

The DoD faces a credible and complex cyber threat from both state and non-state actors. The state-to-state threat can be deterred through the typical array of inter-governmental instruments such as diplomatic, economic and informational instruments of power. However, non-state actors pose a much more unpredictable and dangerous threat because they do not adhere to the legal, moral, and ethical provisions that states tend to

observe.[47] This gives a willing opponent a distinct advantage in their ability to conduct uninhibited cyber-attack campaigns against US cyberspace. Combating these attacks requires an array human and technological capital, neither of which is unlimited. Presently, the DoD is further reducing its possible resources by limiting the talent pool it can select from. Thus, the argument will be made that this in turn limits the effectiveness of how it fights adversaries in cyberspace. This study provides a possible solution in the form of a "militia-like" volunteer organization by facilitating a discussion on the make-up of similar organizations both in the US and around the world.

Organization of Study

The following study is organized into four main parts: a review of current literature, a description of the analysis methodology, an analysis section, and finally a recommendations and conclusions. An in-depth review of the literature pertaining to this research follows this introduction.

[47] Brenner and Clark, *Civilians in Cyberwarfare: Conscripts*, 16-17.

CHAPTER 2

LITERATURE REVIEW

The purpose of this research is to assess the viability of a “militia-like” cyber organization within or controlled by the DoD in order to quickly and more cost effectively supplement the current US government cyber workforce. Computer based network groups are not a new phenomenon in cyberspace. Ever since the Internet was privatized and the World Wide Web was unleashed for public consumption, there have been groups in one form of another interacting in cyberspace. As the Internet has grown so has the fiction and non-fiction literature that details its story. A basic Library of Congress search engine query on the word ‘cyber’ will net you over 1,400 titles published in the last thirty years, the majority of which were written in just the past ten. In general, cyberspace literature can be broken down into three parts: the domain and its capabilities, vulnerabilities and threats, and how to protect or in some cases combat them. For example, book authors typically defined the cyber domain, described its capabilities, provided anecdotal evidence of its vulnerabilities, described the various technical, social, political, and economic challenges that needed to be addressed and then prescribed possible solutions. These solutions vary from intervention at the highest levels (i.e. new US laws and international policy) to possible lower level technical solutions (i.e. duel authentication) as ways to address some of these challenges. The volume of post 1996 era of cyber literature increased by an order of magnitude (from 20 to over 300) in a twelve year period. Collectively these works feature a “flashing neon sign” composition as each author tries to impress upon the reader just how important this new thing called cyber warfare is. However, the researched performed for this paper focused on the literature

from the previous five to seven years emphasizing cyber force response to cyber-attacks. The most prominent source of information on cyber militias was from various Internet sources that ranged from well-known newspapers such as the *New York Times* to Internet blogs from lesser-known entities. Journal and magazine articles represented the next tier of viable information, along with reports from various studies and previous academic papers on similar topics.

This chapter briefly summarizes the opposing views of the cyber threat as well as its capabilities and vulnerabilities currently discussed in literature. Next, a historical overview of militias within the US is provided and includes a brief discussion on Naval privateering after the American Revolution. Current US cyber organizational structure is then detailed with a focus on how the DoD is structured in order to understand where a cyber militia might best fit. Next, a summary of current cyber militias and what they do is reviewed to better understand the context of why they were formed. Finally, a brief overview of possible cyber militia missions and the current cyber law that may or may not be needed to allow these missions will provide an initial assessment of the practicality of a volunteer cyber defense force. This chapter concludes with an assessment of the information gaps and recommendations on how those gaps can be filled to conclude the study.

The Cyberspace Domain and the Threats Within

In ancient Greece, the name for someone who would have steered a ship while traversing the sea was a *Kuberman* and their steersman profession was aptly named *kybernetics.* Several thousand years later in the 1940's, mathematician Norbert Weiner took the prefix "kyber" or "to steer" and morphed it into the prefix "cyber" as a way to

describe his "cybernetic" theories on the communication required to control machines.[48] Simply put, Weiner saw cybernetics as a way to steer electrons from one point to another. Forty years later in 1984, William Gibson first used the term *cyberspace* in his science fiction novel entitled, *Neuromancer*, to describe the futuristic virtual space in which people went about what they thought were normal lives. Cyberspace thus took on a meaning for those living in the 1980's and early 90's as a thing involving possible futuristic concepts but mainly considered these ideas as implausible or science fiction. Since its inception into lexicon thirty years ago, cyberspace has been defined in some manner nearly 20 different ways.[49] Franklin Kramer's book on *Cyberpower and National Security* from 2009 compared fourteen different definitions before arriving at yet another one:

> Cyberspace is a global domain within the information environment who distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[50]

This definition of definitions describes cyberspace as an operational space used by humans to create effects in the other domains (land, sea, air and space) and is a good starting point in understanding why cyberspace has been deemed, "the fifth domain."[51]

---

[48] Paul McFedries, *The Complete Idiot's Guide to Weird Word Origins* (Indianapolis, IN: Alpha Books, 2008), 38-39, Google Books, accessed 6 February 2015, https://books.google.com/books.

[49] Library of Congress, "Search engine result on the word cyber," accessed 3 December 2014, www.loc.gov.

[50] Kramer, *Cyberpower and National Security*, 28.

[51] Ibid.

JP 3-12(R), *Cyberspace Operations*, expands the one sentence definition above into a seven-sentence paragraph that details cyberspace as a domain consisting of three primary layers: the physical network, the logical network and cyber-persona. JP 3-12(R) describes in a bit more detail the interactions between technology and the warfighter in order to relate cyberspace better to the other four domains. The literature review produced a variety of cyberspace definitions, but for the purposes of this study, the JP 3-12(R) definition is used primarily as a way to logically answer the research questions given the scope of this study. However, the eclectic array of definitions exemplifies the complexity of understanding the cyberspace domain and may be a portentous omen when attempting to answer how to best defend against the threats within it.

The literature review confirmed that there is a viable threat to DoD Information Networks (DoDIN). Hacking into the DoDIN via the internet is just one course of action an enemy can pursue as all DoD weapon systems and the data they contain have a physical footprint (facilities, hardware, and wiring) that can be exploited. Whether it is authorized or unauthorized access, the most dangerous of the state and non-state actors will look to gain access through all three layers of the cyberspace domain. The literature review of the cyber threat was comprehensive and by far the most published topic on cyberspace. The review provided numerous definitions, examples and adversaries, all of which have helped frame the complex nature of the cyberspace threat.

Is The Cyber Threat Overblown?

There are others who have argued that the cyber threat is over blown and cite the fact that no was has yet to die at the other end of a keyboard.[52] Bill Blunden and Violet Cheung argue that cybersecurity companies have expertly used their public relations savvy in unnecessarily heightening personal and government angst over the cyber threat. All the doomsday scenarios are not intended to provoke rational thoughts and they believe there is, "a very real effort afoot to create the perception of an imminent threat," to incite the public's fear so they will do or, "pay anything to make the anxiety go away."[53] Blunden and Cheung may have a point as a simple search on Amazon.com using the keywords, "cyberwar," "cyber threat," or "cyber security" will return over 500 titles consisting of an array of books, reports, papers, and even some fiction. More impressively, this is all just within the last 20 years with an amazing 70 percent of those in just the last six years. This suggests a high level of public interest and corresponds with the Stuxnet attack. Every cyber book reviewed after 2009 references in varying detail Stuxnet. It is simply the *Ostrfriesland* of our time. This time around however, instead of Billy Mitchell touting the success of airpower, virtually anyone with some degree of computer background has put pen to paper in an effort to tout the cyber threat. Blunden and Cheung examine Stuxnet and the majority of the highly publicized cyber-attacks over the past several years as well. Their conclusion differs however, in that they

---

[52] Bill Blunden and Violet Cheung, *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware Industrial Complex* (Chicago, IL: Trine Day, 2014), Kindle Edition.

[53] Ibid., 330-331.

consider these events more criminal by summarizing, "We didn't however, encounter any cyber incidents that could be interpreted as cyberwar."[54]

Additionally, there are some who argue that a doomsday cyber-attack would have to be so complex and expensive that it would be cheaper and simpler to just bomb or physically render a target useless. For example, Martin Libiski, a senior executive at the RAND Corporation countered James Clapper's "9/11" characterization of a cyber-attack. "A cyber-attack in and of itself," Libiski concluded, "does not demand an immediate response to safeguard national security. As of yet, no one has died from a cyber-attack."[55] What Mr. Libiski says is true (at least that we know of) but there have been several close calls to include the Baku-Tiblisi-Ceyhan pipeline explosion caused by Russian hackers in 2008 that injured two workers.[56]

Furthermore, 2014 was actually one of its better years in terms of cyber security in recent memory for the DoD. Despite its various networks being attacked an average of 10 million times a day, it has currently not admitted to any vast intrusions or major disruptions. This recent success did not come cheap however, with FY14 setting another record for dollars spent by the DoD on cyber security measures, and while the majority of

---

[54] Ibid.

[55] Kim Zetter, "Tone Down the Cyberwarfare Rhetoric, Expert Urges Congress," *Wired*, 3 March 2013, accessed 3 April 2015, http://www.wired.com/threatlevel/2013/03/tone-downcyberwar-rhetoric.

[56] Jordan Robert and Michael Riley, "Mysterious '08 Pipeline Blast Opened New Cyberwar," *Bloomberg*, 10 December 2014, accessed 11 April 2015, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

career fields in the various services drawdown, cyber employment went up.[57] On the other hand, the private sector had its worst cyber defense year ever and 2014 has been labelled as, "the year of the breach."[58] General Martin Dempsey, CJCS, recently stated that, "While military cyber defenses are formidable, civilian infrastructure and businesses often are targeted first and present a significant vulnerability to our nation."[59]

The opposing view represents a smaller yet valid argument that though the cyber threat is indeed real, its viciousness has been overstated. The increased price tag for cyber security is diverting resources from other US government programs and is benefiting defense and private sector cyber security companies tremendously as it is now a 100 billion dollar a year industry. The opposing point of view alerted the author to various sources that had direct or indirect ties to cyber security companies and ensured questionable data was corroborated with other sources.

Militias Past and Present

The Anti-Federalists and Minutemen of the colonial days were formed to protect isolated towns from Native Americans and then eventually as a quick reaction force to fight and harass the British Army during the American Revolution. These civil-reserve

---

[57] US Cyber Command, "Factsheet," Stratcom.mil, March 2015, accessed 9 March 2015, http://www.stratcom.mil/factsheets/2/Cyber_Command.

[58] Jay Johnson, "If 2014 Was the Year of the Data Breach, Brace for More," *Forbes*, 2 January 2015, accessed 2 February 2015, http://www.forbes.com/ sites/danielfisher /2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more.

[59] Lisa Ferdinando, "Dempsey: Cyber Vulnerabilities Threaten National Security," *DoD News*, 21 January 2015, accessed 13 February 2015, http://www.defense.gov/news/newsarticle.aspx?id=128001.

militias were used as the bulk of the fighting force during the Revolution with the small professional force known at the Continental Army utilized as experts to hone military skills.[60] The Continental Army was known as the "dual army" and it was successful in displacing the King's men from America's shores before being broken down into their singular entities once the war ended. Distrust in a large standing army provided the impetus for the state militias to once again become the primary defense force.[61] The US Congress rectified this by authorizing a 5,000 strong Army deemed the Legion of the United States. However, after a poor performance in the War of 1812, enough popular sentiment existed for the creation of a standing Army to put the US on par with the rest of the world powers. Forged by the Civil and Spanish-American war, America emerged with a formidable military and was a catalyst for the 1903 Militia Act that officially formed the National Guard and the 1916 NDAA that placed the National Guard under federal control. This professionalization of America's military began to change how militias were viewed.[62] They were no longer seen as the protector of America's towns but rather gun-toting extremists who thought they were above the law. The groups *Posse Comitatus* and *Militia of Montana* (M.O.M.) are recent examples of organizations receiving bad publicity for questioning government officials through more aggressive forms of objection. For example, in February 1983, former Posse member Gordon Kahl

---

[60] Millett, Maslowski, and Feis, *Common Defense*.

[61] Tim Seul, "Militia Minds: Inside America's Contemporary Militia Movement," Purdue University, 1 June 2012, accessed 11 December 2014, http://docs.lib.purdue.edu /dissertations/AAI9808519.

[62] Millett, Maslowski, and Feis, *Common Defense*.

killed two federal marshals (who had come to arrest him) in North Dakota and became a fugitive. Another shootout ensued on 3 June 1983, in which Kahl and Lawrence County, Arkansas Sheriff Gene Matthews were killed. Other members of the group have also been convicted of crimes ranging from tax evasion and counterfeiting to threatening the lives of Internal Revenue Service agents and judges.[63] Posse Comitatus and others believe that they are patriots and are performing their civic duty in upholding the Constitution. The word militia thus can hold a negative connotation for some in the American public, as it conjures up stereotypical thoughts of rural Americans preparing for an enemy sure to never come. This connotation unfortunately translates into the thought of a militia as "unprofessional" at best and perhaps illegal at its worst.

Privateers and Contractors

Along the same line of thought was the Navy's version of a militia, something called "privateering." Privateers were similar to their land based counterparts except that they were not volunteers and participants fully expected to profit from their risky endeavors on the high seas. Privateers were not just paid to escort cargo ships as a way to supplement naval protection but were allowed and encouraged to keep whatever spoils were to be had by capturing attacking pirate vessels. Privateering numbers as shown in table 1, show just how effective they were at supporting the Navy during the colonial era.[64]

---

[63] Seul, "Militia Minds."

[64] Haft of the Spear, "INFOSEC Privateering as a Solution to Cyberspace Threats," 6 April 2014, accessed 5 January 2015, http://www.haftofthespear.com/buccaneer-com.

Table 1. Summary of Privateering Numbers

Equipment/Results	US Navy	Privateering Ships
# of Ships	64	1,697
# of Guns	1,246	14,872
# of Enemy Ships Captured	196	2,283

Source: Haft of the Spear, "INFOSEC Privateering as a Solution to Cyberspace Threats," 6 April 2014, accessed 5 January 2015, http://www.haftofthespear.com/buccaneer-com.

Privateering was critical in protecting American security interests at a time when it could not do so on its own. Interestingly enough, America has used this model throughout its history. Most recently, a company named Black Water, was part of operations in the Global War on Terror. Privateers are now called contractors and though effective, did not come without controversy. Contractors fell into a gray area of LOAC and established rules of engagement because they were not under Title 10 or Title 32 when performing "security like" duties in Iraq and Afghanistan.[65] What this simply means is that there may have been a precedent set that allows atypical combatants legal authority in a cyber fight, making, "privateering in cyberspace a way to exercise national power."[66]

From the Minutemen of Massachusetts, to the Naval privateers of the 18th century, and now the soldiers and airmen of the National Guard: there is a rich US history

[65] Ibid.

[66] Ibid.

of citizens forming together for the common defense of the country. Just as militia history in not entirely new, neither is the idea of a cyber militia, as Donald Sheppard first offered the idea of using the National Guard as a "Cyber-Guard" in 1997.[67] Understanding this history allows for the progression of a discussion on just what a cyber militia is and how they might be used in response to the increased threats faced in cyberspace.

Cyber Militias

Just what is a cyber militia? Rain Ottis, founding member of the Estonian Cyber Defense League (CDL) and cyber security expert, has defined it as, "A group of volunteers who are willing and able to use cyber-attacks in order to achieve a political goal."[68] Ottis, is most likely referring to the Russian cyber militia attacks taken against his country to persuade them not to re-locate a Soviet era statue. Thus, the definition Ottis provides suggests that a militia is only used in "cyber-attacks" or offensive operations rather than in the defense or "active defense" as suggested by others such as Troy Mitchell.[69] In the spring of 2015, there were at least seven state-sponsored active cyber militias (Albania, Estonia, India, Iran, Pakistan, Switzerland, and Syria) officially

[67] Donald W. Shepperd, "Cyber-Guard," *National Guard* 51, no. 4 (April 1997): 36-7, accessed 7 October 2014, http://search.proquest.com/docview/231895457? accountid =28992.

[68] Rain Ottis, "Proactive Defense Tactics Against Online Cyber Militia," Academic Conferences International, July 2010, accessed 20 October 2014, http://search.proquest.com/docview/869507133?accountid=28992.

[69] Troy Mitchell, "Cyber Militias," *Marine Corps Gazette* 98, no. 6 (June 2014): 69-72, accessed 27 September 2014, http://search.proquest.com/docview/ 1534474230?accountid=28992.

sanctioned by their parent government.[70] Several other countries are strongly considering them (Turkey) and still others that have them and will not acknowledge their existence (China and Russia). An in depth look of specific types of cyber militias and their key traits will be assessed in chapter 4. However, an overview of the general types or "forms" a cyber militia can take, along with some general historical background will serve to frame the significance of the differences in order to ascertain advantages and disadvantages of current cyber militias.

Rain Ottis has structured cyber militias into three types: the forum, cell and hierarchy. Several other authors (Applegate, Mitchell) cite Ottis and then morph his militia model definitions into a hybrid type that better describes a current militia or cyber security organization. The forum model is an ad-hoc online meeting place where members can meet to share tools, discuss ideas, identify targets and coordinate operations. Performed typically via Internet Relay Chat, a forum can serve as a command and control platform for individuals brought together to perform defensive or offensive cyber operations. Large operations (such as the 80,000 involved in the cyber-attacks against Estonia)[71] will break out into smaller groups to coordinate specific actions directed from the larger group. Group members will mostly remain anonymous and for the most part will not know each other in real life. Thus, groups like Anonymous and other ill-intentioned hacking groups perform illegal 'offensive' actions in a forum. Forums can grow quickly and can therefore mount large operations quickly. However,

[70] Applegate, *Leveraging Cyber Militias*.

[71] Ottis, "Proactive Defense Tactics Against Online Cyber Militia."

command and control is limited and typically takes several leaders identified by prowess or motivation to successful execute forum-based operations.[72]

The cell model is a small group or even just a single individual who are considered experts in hacking. Cell members have performed cyberspace operations on their own or with those they know personally and do so for either fun or for compensation. Cells can mobilize quickly and are extremely hard to infiltrate since they typically know each other. Cells however lack the scalability required to mount some of the more damaging cyber-attacks feared by security professionals. Additionally, due to their small size they have an increased risk of being tracked down as their attacks are analyzed and eventually attributed.

The final cyber militia model is the hierarchy and is described by Ottis as the military model based on its top-down structure of control. Orders are given by an acknowledged leader and then relayed or parsed out further based on the size of the operation. This control aspect is why Ottis describes it as the most likely model for a state sponsored group.[73] The hierarchy model benefits from its formal creation as members can train, coordinate, and exercise on regular intervals to harness expertise. This model is also the most reliable as members are typically there for a cause and are getting compensated in some manner (i.e. experience or money).

Taking into consideration these definitions of a cyber militia from Ottis, Mitchell, Applegate and others, I propose a US Cyber Militia definition for the purposes of this

[72] Ibid.

[73] Ibid.

study might be: A group of non-professional fighters with cyber security credentials that gather together in conjunction with current DoD cyber professionals for the common defense of the US Cyber Domain.

"Non-professional fighters," would be defined as volunteers from industry and academia while the "DoD cyber professionals," are the current array of cyber warriors employed the US government. Specifically, Rain Ottis describes a cyber warrior as a professional paid member of a Government employing cyber capabilities in some manner.[74] These individuals are current active duty, reserve, civilian and contractor personnel whose duty encompasses cyber operations as part of an organized command structure. This definition closely resembles the definition of "combatant" according to the Geneva Conventions minus the part of a "visible marking that identifies themselves as a non-civilian."[75] A militia, on the other hand, would be comprised of civilian volunteers, perhaps under some form of command structure but not necessarily, and would again not be visibly marked. The current operating nature of the cyber domain allows for anonymity to an extent the LOAC could never have considered, and specifics of how to possibly address this will be analyzed later in this thesis.

With an understanding of what a cyber militia is and what it could conceivably be defined as by the US government, the following sections will discuss current US cyber operational structure, where a militia could possibly fit and the role it may perform.

---

[74] Ibid.

[75] Geneva Convention, *Relative to the Treatment of Prisoners of War,* 12 August 1949, 6 UST. 3316, T.I.A.S. 3364, 75 U.N.T.S. 135, Article 4A1-4A3.

DoD Organizational Cyber Structure and Operations

Current DoD policy and doctrine was reviewed to build an understanding of the current military organizational structure and cyberspace operational concept. Additionally, National level cyber security strategy and operating concepts were reviewed to understand how the DoD fits into the grand scheme of US cyber security strategy. In general, the DoD operates two of six federal cyber centers known as the Defense Cyber Crime Center and Joint Task Force-Global Network Operations. These six centers feed the National Cyber Security Center, which then fuses all the information into a high-level picture for the development of national cyber security responses and strategy.

The DoD strategy for operating in cyberspace is to treat cyberspace as an operational domain, employ new defense operating concepts, partner with other US government departments, build robust international relationships, and leverage the Nation's ingenuity through an exceptional workforce and rapid technical innovation.[76] This strategy is executed through three cyberspace mission areas: 1. Defend the Nation; 2. DoDIN Operations and; 3. Combatant Command (CCMD) Support. DoD activities supporting these mission areas are composed of the military, intelligence, and ordinary business operations required to implement the strategy described above.[77] DoD cyberspace operations strive to enhance operational effectiveness while leveraging various capabilities from physical domains to create effects in support of combatant

[76] Department of Defense, *Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, April 2015).

[77] Ibid.

commanders through US Strategic Command (USSTRATCOM). US Cyber Command (USCYBERCOM) is a subordinate command to USSTRATCOM and executes the three mission areas through three corresponding Cyber Mission Force (CMF) teams.

1. The National Mission Force (NMF) secures, operates, and defends DoD networks. Specifically, the NMF is a counter-cyber force to stop cyber-attacks and malicious cyber activity of, "significant consequence against the Nation."[78]

2. The Combat Mission Force defends the Nation in cyberspace and is designed to support CCMDs in carrying out approved operational plans and contingency operations with integrated cyber effects.

3. The Cyber Protection Force (CPF) supports the Combatant Commander (CCMD) full spectrum operations in cyberspace. The CPF is divided into four mission areas: National, DoD Information Networks (DoDIN), Combatant Command (CCMD) support, and Service support. All CPF units are focused on actions internal to the defended network, which primarily is within the DoDIN unless they are separately authorized to defend non-DoD networks. The core capabilities of these teams are mission protection, discover and counter infiltration, cyber threat emulation, cyber readiness, and cyber support. These teams integrate and synchronize cybersecurity functions such as assessments of network vulnerabilities, penetration testing, remediation of vulnerabilities, and hunting on networks for adversary activity.

Once fully manned, trained, and equipped (FY2018), these 133 teams comprising the CMF will execute the three primary missions with approximately 6,200 military and

[78] Ibid.

civilian personnel along three main lines of operation: (1) DoDIN Operations; (2) Defensive Cyber Operations (DCO) and; (3) Offensive Cyber Operations (OCO). Each service component then supports the cyber mission by ensuring the integrity of their own cyberspace with a combined force of more than 50,000 military, civilian and contractor personnel. Second Army, 24th Air Force, 10th Fleet and Marine Force Cyber perform service cyber missions out of various locations across the US. Each service states its mission slightly different but in general, they plan, coordinate, integrate, synchronize and conduct activities to direct the operations and defense of DoDIN capabilities in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to adversaries.[79] Figure 1 depicts the USCYBERCOM organizational structure.

[79] Ibid.

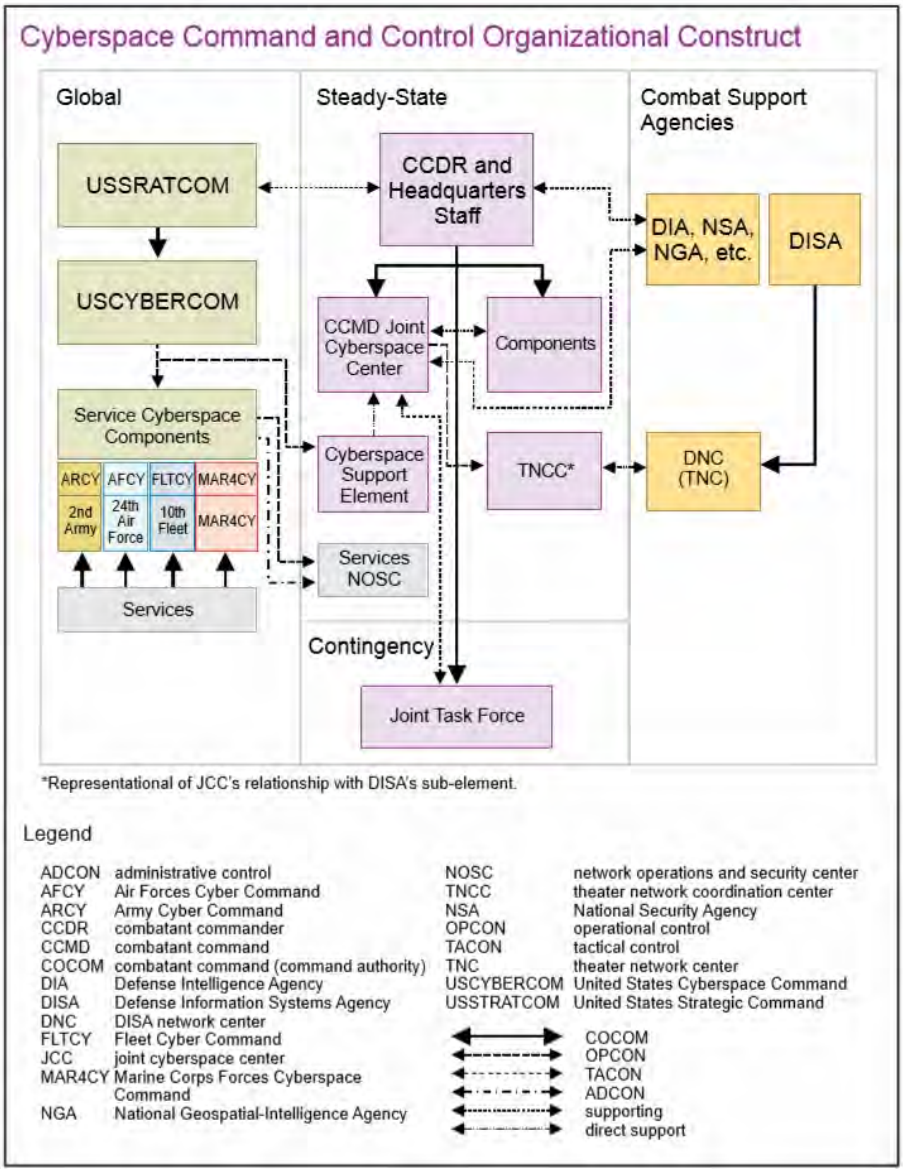

Figure 1. DoD Cyberspace Command and Control Structure

Source: Chairman, Joint Chiefs of Staff, Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington, DC: CreateSpace Independent Publishing Platform, 2013).

Due to the limitations described in the introduction of this paper, the remaining discussion on DoD cyber force structure will focus on DoDIN and defensive cyber operations. The DoD is primarily responsible for its own information networks known as

the DoDIN, the defense of which falls primarily to the Defense Information Systems Agency (DISA), and the CPF teams (CPTs) described above. The CPTs that comprise the CPF conduct tailored cyberspace defense for specified missions of varying intensity and duration. Their key functions are mission protection, focused monitoring, detection of advanced threats and cyber force mission readiness. Specifically the CPTs provide comprehensive risk mitigation of DoD cyber terrain and focus on fortifying force posture and process from the inside out. The CPTs also hunt for and illuminate adversary activity within the DoD and provide adversary-like engagement as a cyber aggressor force or "OPFOR" (opposing force). These teams are the compliance and operational ready experts that inspect, recommend, and direct policy implementation and change.

In summary, the literature of current US government cyber infrastructure, policy, and strategy was comprehensive and provided an excellent high-level overview of how the US is working to maintain cyberspace dominance. The current literature provided sufficient knowledge to assess the various roles and responsibilities between the departments and USCYBERCOM's mission force teams to suggest where and how a volunteer force may best serve. Several authors have suggested possible missions and roles for such a force and are summarized in the following the section.

Roles and Mission of a US Cyber Militia

There is a moderate amount of literature on how several countries have used cyber militias as part of their cyber operations but little has been written on how the US might successfully employ one. Several authors (Rosenzweig, Kramer) mention US cyber militia utilization briefly (no more than a page or two) in their respective books while several others (Harding 2012, Mihevic 2012) have written three to five page Internet

articles on the subject. There is currently just one published book on cyber militias and is entitled, *Cybermilitia: A Citizen Strategy to Fight, Win and End War in Cyberspace.* Written in 2013 by Siobhan MacDermott and J. R. Smith, they argue that it is past time for the US Government to stop worrying about over regulating the private sector and to impose laws required for our security, to include standing up a cyber militia.[80] MacDermott has been described as one of the foremost experts on future information technology and the thesis of her book calls for a national return of values that existed at the founding of the US. Specifically, the revaluation discussed throughout the book takes the form of a cyber militia, not organizationally, but as a state of mind, an attitude, and as a set of behaviors. MacDermott sees the cyber militia as a social contract that provides an essential means to the common defense and self preservation of the country. She concludes that a cybermilitia is, "A redefinition of citizenship with respect not only to the nation, but also to humanity . . . the concept of the cybermilita offers possibilities far richer than protection."[81]

Another extensive resource on cyber militias is several works from Scott Applegate to include "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations." This 2012 paper provides a great overview of current state and non-state sponsored militias, how they might be formed, and how Western countries such as the US might utilize them as part of their overall cyber strategy. Applegate's thesis is that to

---

[80] Siobhan MacDermott and J. R. Smith, *Cybermilitia: a Citizen Strategy to Fight, Win, and End War in Cyberspace* (Birmingham, MI: IT-Harvest Press, 2013), Kindle Edition.

[81] Ibid., 115.

combat non-state, unconventional attackers in cyberspace, state actors should consider unconventional means to counter these forces.[82] Applegate makes the classic case of "fighting fire with fire" in that in order to be successful in cyber operations one must consider all available means. Applegate offers a slight caveat to his thesis with concern to limited resources as militias are for the most part formed due to lack of resources (be it funding or personnel) to stand up a regular force. Throughout his paper, Applegate uses examples of the vast amount of expertise that is available in Western countries to combat non-state cyber aggressors but are not used because of self-imposed legal, moral, and ethical constraints.[83] However, the same can be said about how Western countries and specifically the US fights its land, sea, air and space "wars;" the decision to fight limited wars against opponents that are using total war strategies. This will most likely not change unless US leadership perceives that US security interests are at risk. Using the current US military cyber organizational construct as a baseline, several authors have suggested roles and possible missions for a US cyber militia within such a construct. Troy Mitchell categorized cyber militias into clan, cell and state-sponsored entities of which each can perform an array of cyber functions.[84] Specifically, a militia with the right command and control structure could be raised quickly through cyberspace to either combat the attack or provide a form of attribution or counterattack. The counterattack or "active defense" strategy suggested by Mitchell was also highlighted by a group of

[82] Applegate, *Leveraging Cyber Militias*.

[83] Ibid.

[84] Mitchell, "Cyber Militias."

NATO experts that were given the task of determining possible measures to deal with cyber-attacks.[85] Specifically, the design of an active defense strategy is to improve cyber security by stimulating reactions of the threat agents to increase situational awareness.[86] By looking "over the wall" new information is now available that provides strike options and enhanced operational preparation of a real or virtual battle space.

A 2007 compendium of papers from the NATO Science for Peace and Security advanced workshop entitled, "Responses to Cyber Terrorism," concludes that there is a cycle of five defense measures required for cyber security. On this list includes the formation of quick response teams available to respond to cyber incidents 24 hours a day.[87] Additionally, this publication defines cyber terrorism, discusses the need for international cyber laws, and goes into detail on the Estonian cyber-attack and subsequent defense in 2007. However, the most useful information is the summary of the discussions that answered the following questions:

1. What measures might disrupt terrorists use of the internet?

2. What measures might be taken to deal with cyber-attacks?

3. What security measures might protect against cyber terrorism?

Possible personnel related answers to these questions were to establish "neighborhood watch type" programs, build a cadre of capable defenders to re-route or

---

[85] Lee Jarvis, *Center of Excellence Defence against Terrorism*: *Responses to Cyber Terrorism* (Amsterdam, NLD: IOS Press, 2008), ProQuest ebrary, accessed 1 November 2014, http://www.tandfonline.com/doi/abs/10.1080/1057610X.2014.853603#.U2AZtfldXDs, 144.

[86] Ibid., 145.

[87] Ibid., xi.

fix connections, establish active defenses to punish the attacker ("hack back"), and provide "noise" in known terrorist chat rooms. What was not discussed was who specifically they meant by "capable cadre" or who might be best suited to employ the proposed defense measures. Personnel are just one aspect of a successful cyber defense (equipment, access and training being the others) and a possible subset of that is an organized militia.

Ottis further describes his militia models in terms of what they can do offensively, which limits the usefulness of his examples for the purposes of this study. However, Applegate extended the Ottis models by specifying which ones might be best suited for a nation-state, understanding a democratic government would most likely not have approval to use a cyber militia in a preemptive manner.[88] For example, a forum to Applegate would be a gathering of cyber security professionals to review code for vulnerabilities and then distribute any findings to a national cyber center or directly to a company itself. In fact there are companies that sponsor this type of activity through "bug bounties" in which reviewers are rewarded with free software or recognition.[89] Applegate addresses the downside of a state-sponsored forum, which is that members would be limited to non-combative activities since they would have no combatant status under LOAC.[90] Applegate believes that any lawful roles of a cyber militia in a democratic state would be limited in part to LOAC obligations and the vetting process that will most

---

[88] Applegate, *Leveraging Cyber Militias*, 10.

[89] Microsoft, "Bug Bounty Programs," 23 September 2014, accessed 20 April 2015, https://technet.microsoft.com/en-us/security/dn425036.

[90] Applegate, *Leveraging Cyber Militias*, 12.

assuredly be required by lawmakers. However, Applegate still sees a "force multiplier" type of role through activities such as open source information infrastructure mapping of a known entity's networks, websites, and service providers. Such an act was accomplished by the Cyber Security Forum Initiative (CSFI), a 17,000-member private/non-profit group formed via LinkedIn in a 2011 cyber campaign against the government of Libya. The results were provided in a report to the US Government to support both kinetic and non-kinetic engagements in operation Odyssey Dawn.[91] Applegate highlights actions from a variety of militia types, all of which exemplify the defensive or active defense type of roles previously described.[92]

Opposite this line of thinking, Mihevic argues that cyber militias would be more effective in offensive roles. The defense of US national technology and critical infrastructures requires the close coordination of public and private sectors and the implementation of executive authority. A cyber militia simply cannot provide the form and accountability required for a defensive role.[93] Offensive operations are not bound by these requirements and cyber-attacks often benefit from their lack of structure and diversity of attack vectors, features cyber militias readily provide. Cyber militias can be assigned a target or objective and given the ability to freelance and choose their methods

[91] Ibid., 23-24.

[92] Ibid., 7-24.

[93] Jake Mihevic, "Cyber Militias in the US: Feasibility, Structure, and Purpose," InfoSec Island, 21 August 2012, accessed October 2, 2014, http://www.infosecisland.com /blogview /22164-Cyber-Militias-in-the-US-Feasibility-Structure-and-Purpose.html.

based on their group capabilities. The absence of formal rules of engagement allows the cyber militia to exercise creativity and innovation in developing attack methods.

The literature review produced varying opinions on the roles and missions a cyber militia might best be able to perform. In a vacuum, it seems as though a freelance group of experts, given a high degree of freedom to maneuver, could offensively exploit the nature of the cyberspace domain. However, the reality of public, political and legal opinion will ultimately dictate how a militia is utilized in a Nation-State such as the US.

Legal Overview

This paper will not attempt an in-depth review of the current legal issues concerning cyberspace. Rather, a general overview of the legal aspects most pertinent to this study are briefly summarized to provide the reader an idea of what US and international laws might need to change for the proposed cyber militia to exist. Specifically, what government entity can raise a militia? What would constitute their usage? And has US or international law defined what a cyber-attack is?

Legal research on the subject of militias was performed to verify the Federal Government's authority to organize such an entity. Article 1, Section 8 of the Constitution of the United States provides that:

> The Congress shall have the power. . . . To provide for calling forth the militia to execute the laws of the Union, suppress insurrections and repel invasions…To provide for organizing, arming, and disciplining, the militia, and for governing such part of them as may be employed in the service of the United States, reserving to the states respectively, the appointment of officers, and the authority of training the militia according to the discipline prescribed by Congress.

Additionally, the Second Amendment reads: "A well regulated militia being necessary [for] a free State, the right of the people to keep and bear arms shall not be

infringed." The Constitution, therefore, demonstrates that militias are a creature of the state, subject to being called forth by the U.S. government "to execute the laws of the Union." This is bolstered by the wording of the Second Amendment which holds, "A well regulated militia being necessary [for] a Free State" and by Article 1, Section 8, Subsection (16), which reserves to the states "the appointment of officers and the authority of training the militia." Thus, the research has confirmed the US government's authority of raising a militia but now the question becomes under what international law can such a militia (or any force) be utilized to repel cyber-attacks?

What constitutes a threat is governed by Article 2(4) of the UN Charter as it provides that member states "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[94] Oona Hathaway and her group of law researcher as the University of California noted that, "Weaker states and some scholars have argued that Article 2(4) broadly prohibits not only the use of armed force, but also political and economic coercion. Nonetheless, the general consensus is that Article 2(4) prohibits only armed force." Discussions about cyber-attacks have the potential to reignite debates over the scope of Article 2(4). Because it is much less costly to mount cyber-attacks than to launch conventional attacks, and because highly industrialized states are generally more dependent upon computer networks and are more vulnerable to cyber-attacks: cyber-attacks may prove to be a

[94] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber Attack," *The California International Review* (Summer 2012), accessed 26 April 2015, http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf.

powerful weapon of the weak. This change in the cost structure of offensive capabilities may both increase the likelihood of cyber-attacks and change the political valence of different interpretations of Article 2(4)'s scope. Stronger States may begin to favor more expansive readings of Article 2(4) that prohibit coercive activities like cyber-attacks. At present, however, the general consensus remains that Article 2(4) prohibits only physical armed force.[95]

The next logical question then is to ask if a cyber-attack is considered physical force. To do this, an agreed to definition of a cyber-attack must exist, which it currently does not both internally to the US and internationally. The DoD, DHS, DoS and US National Research Council all have varying definitions. Additionally, various international organization also have varying definitions such as the Shanghai Cooperation Organization, a security cooperation group composed of China, Russia, and most of the former Soviet Central Asian republics, as well as observers including Iran, India, and Pakistan.[96]

A brief review of US law reveals that technically a US cyber militia could be raised in defense of the country. However, what constitutes a threat in cyberspace remains nebulous at best. There is currently no national or international definition of a cyber-attack and whether or not such an attack would give a nation-state the authority to respond in force, be it kinetically or non-kinetically in any of the domains. This

[95] Ibid.

[96] Ibid.

ambiguity is what gives authors on the topic of a cyber militia the most concern and is discussed briefly in the next section.

Constraints

The literature revealed that the largest concern by authors on the subject of establishing a cyber militia in a democratic nation-state are the legal constraints imposed by lawmakers. Mihevic argues that the primary challenge to the feasibility of a US cyber militia is legal and the risks of a cyber militia stem from a lack of control over the membership.[97] Even in a hierarchy, the most formal of the forms described by Ottis, have little effective control afforded to leadership. The are many opportunities for a cyber militia member, or entire cyber militia for that matter, going "rogue," and exhibiting behavior the US is attempting to establish as internationally prohibited. Mihevic summarizes that, "It is not advisable for a nation to be affiliated with a cyber militia unless there is a hierarchical structure and military oriented vetting procedures. Without such safeguards, a militia may provoke conflict or take actions averse to the nation's interest."[98]

An additional constraint will be imposed in some manner by public opinion and the political decisions they drive. Joel Harding makes the point that tendencies exhibited by US lawmakers and public sentiment may prohibit such an organization such as, "the nature of US culture is paranoid, cynical and negative. We tend to micromanage; unless

[97] Ibid.

[98] Ibid.

we can physically check to see someone's weapon is in a safe or in a holster, we tend to disbelieve they have adequate security on a weapon."[99]

The literature review showed that there are legal and political implications that need to be taken into account by the NCA if and when a cyber militia is considered. These constraints will be further discussed and analyzed in chapter 4.

Literature Summary

In summary, over 70 cyber security related pieces of literature have been reviewed for this study to include recently published journal and electronic news articles, government reports, previous cyberspace related studies, and current US Government law and military doctrine. These resources have ranged in topic from the growth of the cyber threat and how current cyber militias are being used, to specific US law that might allow for a US cyber militia. These articles provide an array of possibilities to combat cyber threats but little evidence of how those suggestions might impact or have impacted cyber-attacks. For example, Jake Mihevic's three-page online article is one of five that briefly touch upon the use, make-up, and feasibility of cyber militias and though the discussions are not to the depth of the Applegate paper or the MacDermott book, they provide varying perspectives on the topic.[100] The literature review confirms that there is a great deal of current and relevant cyber warfare literature but very little when it comes to discussing democratic state sponsored cyber militias and their impacts on offensive and

[99] Joel Harding, "Thoughts on a US Cyber Militias," InfoSec Island, 23 August 2012, accessed 1 October 2014, http://www.infosecisland.com/blogview/22224-Thoughts-On-a-US-Cyber-Militia.html.

[100] Mihevic, "Cyber Militias in the US."

defensive cyber capabilities from the military's perspective. There is a moderate amount of cyber militia literature concerning other countries but only a few address specifically the impact they might have (be it positive or negative) in the US, or provide a current military perspective. These references also do not detail how a cyber militia might be viewed from the American public, the international community or the DoD. In fact, the largest information gap is the "cyber warrior" perspective concerning anything to do with a militia. Understanding how a militia might affect the efforts (good or bad) of a conventional force has yet to be discussed.

The literature review also confirms that due to a lack of quantitative data, a qualitative study is currently the only feasible approach to study cyber threats and the means to combat them. The following chapter provides an explanation of the analysis methodology used in this study to answer the primary and secondary research questions. The subsequent chapter then details each component before providing a set of findings and recommendations for the reader's consideration.

CHAPTER 3

METHODOLOGY

The primary purpose of this study is to examine the key traits of worldwide cyber militias, organizations, and associations to determine if a similar volunteer framework could be a cost effective augmentation to regular US cyber forces. This chapter outlines the methods used to answer the primary research question as well as the secondary questions proposed previously in chapter 1.

The literature review confirmed that due to a lack of quantitative data, a qualitative study is currently the only feasible approach to study cyber threats and the means to combat them. This is not for lack of trying but rather the nature of the current cyber operating environment; it is difficult to create metrics that correlate the effectiveness of one defense versus another. The DSB was charged to create such a set of metrics but conceded that it was too difficult to do in the timeframe allotted for its research.[101] The DSB instead provided a top-down driven framework that calls for commonality between systems and network components.[102] Interpreted another way, one could argue this is a call for standardization or perhaps a normalization among DoD networks to ensure possible metric systems are comparing and reporting on the same levels of security. The lack of metrics makes quantitative analysis of how a militia might affect US cyber security virtually impossible. Additionally, many attacks go unreported,

[101] Defense of Defense, *Resilient Cyber Systems*, 15.

[102] Ibid.

unnoticed, or do not have a significant impact, so any quantitative analysis would not answer the fundamental research question of the value a cyber militia might provide.

The research is broken into three main parts, the first of which describes and assesses the current cyberspace operating environment through a comprehensive literature review in order to answer the first three secondary research questions. This assessment included an up-to-date cyber threat examination as well as a review of the key issues and constraints surrounding US efforts to combat it. Additionally, as a way to frame the current state, a brief examination of militia history within the US was performed. The second main part of the research dealt with how current cyber militias and similar groups are organized and implemented. A case study of these groups and their key characteristics provides a basis of knowledge in how such a group could be formed in the US. This case study comparison analysis answered secondary research questions four and five. Finally, to answer the final secondary research question as well as the primary research question, a qualitative analysis was conducted of all the information gathered and then summarized into a variety of findings and recommendations in chapter 5.

In summary, the research was qualitative since a key variable missing in conducting a quantitative study is numerical data showing cyber-attacks before and after the formation of cyber militias. This is due to the lack of meaningful metrics in cyber security analysis (both public and private) that measure outcomes of actions performed and the complexity of attacks. This limits the accuracy of resource investment decisions and was a major finding (and subsequent recommendation to fix) in the DSB's study on

resilient cyber systems.[103] The resulting analysis performed in this study compared current state and non-state cyber militias and outlined possible DoD variances by assessing their critical traits and notable successes. Quantitative data is used from secondary sources to substantiate arguments pertaining to scope of the cyber threat, impact of current militias, and cost of either. This was achieved through a comprehensive examination of current literature, archived speeches, and congressional hearing notes. The analysis resulted in a variety of findings and subsequent recommendations identified in chapter 5. The following chapter details the analysis performed.

[103] Ibid., 3-14.

CHAPTER 4

ANALYSIS

> Finally we will want to consider whether and how to engage civilian populations in the response to a cyber insurgency. One can imagine, for example, the development of cyber militias who are recruited by the American government to assist in responding to attacks by non-state actors, like Anonymous. Those sorts of ready reserve militia might be available for defensive measures should an attack of significant proportions ever occur.
>
> — Paul Rosenzweig, *Cyber Warfare*

The purpose of this research is to compare and contrast current cyber militias and their impact on cyberspace operations. The primary question addressed in this study is whether there are efficiencies to be gained in US cyber operations by incorporating a similar volunteer force in some manner. Analysis of the primary research question starts with defining the type of impacts one might expect from a volunteer workforce. However, in order to answer the primary research question, the secondary questions are first explored in as much depth as possible. The first three secondary research questions were answered qualitatively by comparing and contrasting the various sources discussed in the literature review to the published opinions of experts and leaders in the cyber security field. Questions three through six were answered by a comparative case study analysis that took an in-depth look at a variety of current state and non-state cyber militias as well as several other professional cyber security organizations. This chapter discusses the analysis performed in answering the primary research question and the six secondary research questions in order to substantiate the recommendations in chapter five. This chapter works through the subsequent analysis performed in answering those

questions by simply going in numerical order and concludes with a summary that provides a basis for possible recommendations.

The Current Threat to the DoD in Cyberspace

Many have described, defined, and postulated what the current and future cyber threats are and will be. This thesis will not attempt to replicate those efforts. Rather, this paper uses the summary of threats from JP 3-12(R), *Cyberspace Operations,* and Lieutenant General Keith Alexander's characterization of Cyber Warfare as a stepping-stone for discussion. In general, this paper views the cyber threat in two distinct ways; the first being the inherent structure of the cyber domain (specifically the Internet), and the second being the adversaries exploiting that structure. Just as in the other domains, cyberspace has its inherent dangers. But unlike the others, the structure of the domain in completely man made. Cyberspace and specifically the Internet was conceived in such a way that has allowed for unbelievable growth and speed. Known as "open architecture," this system trait is defined by subject matter expert Clifton Erikson as, "An architecture designed to make adding, upgrading, and swapping components easy."[104] It is this additive capability that makes the Internet as powerful as it is. However, this same openness also makes the Internet extremely unsecure and vulnerable to exploitation. As Richard A. Clarke summarized in his book on Cyber War, "The designers of the Internet did not want it to be controlled by Governments, either singly or collectively, and so they

[104] Clifton A. Ericson, *Concise Encyclopedia of System Safety: Definition of Terms and Concepts* (Hoboken, NJ: John Wiley and Sons, 2011).

designed a system that placed higher priority on decentralization than on security."[105] Just as gravity is a danger to an aircraft and the typhoon is to a ship, the environment in cyberspace is a threat itself that must be contended with.

Adding to the inherent danger of cyberspace are adversaries looking to exploit its openness. Examples of these threats, to include specific attacks and the impact they could have on the DoD, are discussed briefly to establish a view of the adversaries in which cyber militias could oppose. In general, the threat in cyberspace is called Computer Network Attack (CNA) but has also come to be known as "cyber warfare" in recent years. Lieutenant General Alexander described cyber warfare as:

> The focus of cyber warfare is on using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability, while protecting our own.[106]

JP 3-12(R) then dissects the "who" of the cyber threat into four adversaries: Nation State, Transnational, Criminal, and Individual or Small Group.[107] A nation state adversary would be currently recognized nation such as China, Russia or Iran. These actors represent the most advanced threat due to their resources and their willingness to exploit the cyber realm to build national power. A transnational actor is a large group bound by an ideology but with no recognized national borders. These can be violent terrorist organizations such as the Islamic State (IS) or Al Qaeda but can also encompass

---

[105] Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: HarperCollins, 2010), Kindle, 31.

[106] Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly,* no. 46 (3rd Qtr 2007): 60.

[107] Chairman, Joint Chiefs of Staff, JP 3-12(R), *Cyberspace Operations,* 19-20.

worldwide diaspora communities, or subcultures within a nation's borders. All of which utilize cyberspace to raise money and support for their causes such as the Indian Cyber Army (ICA). At first blush, the ICA looks like a government entity, but despite its defensive nature in cyberspace, it is actually a private organization that raises money to support its operations. Next are the criminal organizations such as the Russian or American mafias that use cyberspace to make money through a variety of acts that include selling cyber weapons, stealing and selling secrets or personal data, and are most dangerous when used as surrogates by a Government.[108] Russia's *Nashi*, is an example of this and will be discussed further in the case study analysis. Finally, the individual or small group threat is comprised of hackers or hacker cells that look to disrupt and discredit a government through "hacktivism" to serve some cause. The group Anonymous, fits this mold and will be reviewed in the case study analysis.

JP 3-12(R) describes the greatest challenges of the cyber threat as anonymity (inability to connect a cyber-attack to an individual or group), autonomy and trans-regional nature. Imagine a "blue force tracker" with nothing but gray dots on the screen representing all the players on a battlefield. Assessing hostile intent becomes extremely difficult and now each dot must be analyzed over a short amount of time to determine friend or foe. This takes time and just as in the other domains, an attacker or the initiator holds the advantage.[109] Anonymity, however, can work both for and against potential

---

[108] Noah Shachtman, "Kremlin Kids: We Launched the Estonian Cyber War," *Wired*, 11 March 2009, accessed 14 January 2015, http://www.wired.com/2009/03/pro-kremlin-gro.

[109] Ramberto Torruella, "Determining Hostile Intent in Cyberspace," *Joint Forces Quarterly* 75 (4th Qtr 2014): 114-21.

adversaries in cyberspace. For example, opposing forces can slip into one another's command posts (i.e. a chat room) without detection. Militias could expose this weakness by infiltrating an online forum and then either actively or passively counterattacking an ill-intended action by an enemy. These examples demonstrate two key principles of the fight in cyberspace: initiative and anonymity. Interchanging the terms "initiative" and "anonymity" with "offensive" and "surprise," yield two of the twelve principles of warfare.[110] Though there are no officially published principals of cyber war, Brian Kelly, the Chief Security Officer at the network solutions company Rackspace, believes the current principals of war outlined in JP 3-0, *Joint Operations*, serve as a great start. He argues through relevant examples that the current principals of war all apply to cyber war in one manner or another and summarizes, "we believe these principles provide guideposts that anyone can follow to improve the way information security organizations are run." [111] Current worldwide cyber militias exhibit several or more of these principles and have organized to exploit them in some manner.

The list of successful cyber-attacks in just the past five years is exhaustive and thus the current debate in cyber space is not that it is happening but to what scale, to what degree and to what lengths it will evolve. Some argue that there is a doomsday event or "cyber Pearl Harbor" is just around the corner. As Admiral Rogers stated in November

---

[110] Chairman, Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: CreateSpace Independent Publishing Platform, 2011).

[111] Justin Greis, "The Twelve Principles of Cybersecurity Warfare." Art of Advice.com, 6 February 2015, accessed 19 April 2015, http://www.theartofadvice.com /2015/02/06/the-twelve-principles-of-cybersecurity-warfare.

2014, “It’s not *if* a cyber-attack will occur against our power grid, it’s when.”[112] The DSB has described the cyber threat as serious and with, “consequences similar in some ways to the nuclear threat of the cold war.”[113] The catastrophic cyber-attack would be a worst-case scenario that involves the combination of multiple cyber network attacks on critical national infrastructure accompanied by some form of physical attack. The result would be loss of life, a paralyzed government and an increased sense of vulnerability. The Russians provided a peek into what a coordinated cyber-attack might look like when they invaded northern Georgia in 2008. Georgia was assailed through the cyber domain by thousands of DDoS attacks that hindered government network and early warning operations Russian army forces crossed the border. This marked the first time in history that a country was invaded through those three domains at the same time.[114] However, it may be the Chinese that ultimately morphs the cyber threat into an all-encompassing attack. Colonel Qiao Liang and Colonel Wang Xiangsui of the People’s Liberation Army Air Force, published a book entitled, *Unrestricted Warfare* ,which provides a glimpse of how China sees warfare in the 21st century. Their asymmetric theories summarize that a networked world means warfare is no longer restricted to just military means. Rather, modern warfare will include “trade war,” “financial war,” “information war,” “network warfare,” and “technological warfare,” all facilitated by interconnected systems and thus damage from

[112] Rogers, “Cybersecurity Threats: The Way Forward,” testimony.

[113] Department of Defense, *Resilient Cyber Systems*, 31.

[114] Rosenzweig, *Cyber Warfare*, 32.

these types of threats will certainly be greater for a large networked country such as the US.[115]

The Use of Militias by the United States

Historical accounts of how militias were used in the US provide a possible means to end state achievement today when analyzed in the correct context. As military historian David Holden once stated, "History provides a trail of bread crumbs to follow, but never a whole answer," and thus the "how" of militia utilization is not as important as to the "what" or the "why."[116] Simply put, US militia formation was predicated on the basic human instinct of survival. Colonies that did not defend themselves were at a greater risk of harm or capture than those that did. This threat was why militia participation for able-bodied men was not an option; it was required. Militias performed well before and during the American Revolution when survival of the colony and then as a country were in question. This success prompted the newly formed American Congress to retain only a small regular standing army to "garrison the west" and "awe the Indians."[117] Fear of a large standing Army was of course a reason as well and so the preponderance of the fighting force remained to be that of militiaman from the various States and territories. In fact, the militia to "active" force ratio post Revolution was

---

[115] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (New Delhi, India, 1997), Kindle, 31-32.

[116] David Holden, "The Importance of Studying History" (Lecture, History 100 and 300, Command and General Staff College, Fort Leavenworth, KS, March 2015).

[117] Millett, Maslowski, and Feis, *Common Defense*, location 1840.

approximately four to one.[118] Unfortunately, this "composite" force did not perform well. Notable losses to inferior Indian forces prompted the creation of the Legion and started the slow but sure "flipping" of the active to reserve component ratio. The poor performance was due in part to the Uniform Militia Act not imposing training and organizational standards across the states. Additionally, rampant insubordination and desertions played their parts as well. Thus, militia units were not interchangeable between states making them an ineffective fighting force in times of conflicts.[119] What can then be gleaned from early militia activity is that it performed well when there was a credible threat to an established way of life. This is corroborated later in this chapter during the case study analysis when a review of the contextual details of why various worldwide militias were also formed. What history also suggests is that uniformity in training and organizational construct provides greater flexibility across a force as units become interchangeable.

DoD Cyberspace Organization and Operations

Organizing to deal with the threat in cyberspace requires the environmental awareness to effectively generate the capabilities and policies necessary to synchronize national and international security efforts. This awareness has been demonstrated by the NCA as the ever-increasing amount of cyber-attacks has spurred responses in the form of policy development and appropriations to create and support organizations tasked with providing national cyber security. Specifically, the DoD formed USCYBERCOM and

[118] Ibid.

[119] Ibid., 1826.

assigned it the mission of gaining, maintaining, and exploiting advantages within the cyber domain. USCYBERCOM aligns with the typical hierarchical structure attributed to military organizations and executes its operations through a defined chain of command. This unit structure has been described by organizational theorists as, "mechanistic," which is an organization characterized by vertical coordination and high task specialization.[120] These organizations typically struggle to reorganize into adaptive systems that can match the complexity of problems such as the cyberspace threat. However, the traditional strength of a mechanistic organization is to leverage its hierarchical structure to generate mass and thereby gain a position of advantage over an adversary.[121] This strategy has worked for the DoD in the past, as shown in the development of the Army Air Corps during the interwar period and thus, it seems it is doing something very similar today. USCYBERCOM is dealing with cyber threats by employing the traditional mechanistic approach of generating mass[122] but is doing so with the small, specialized teams that are a prerequisite of the hybrid "M-type" organizational model geared to combat complex problems.[123] The NMF and CMF teams, defined in chapter 2, represent a simple, yet innovative approach to utilize an

---

[120] Jennifer L. Miller, "Conducting Business in a Fast-Paced World: The Importance of Change Management," *Student Pulse* 2, no. 10 (2010): 2.

[121] Robert Axelrod and Michael D. Cohen, *Harnessing Complexity: Organizational Implications of a Scientific Frontier* (New York: Free Press, 2001).

[122] Gregory C. Wilshusen, *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*, Report No. GAO-11-75 (Washington, DC: Government Accounting Office, 2011).

[123] Miller, "Conducting Business in a Fast-Paced World," 6.

organization's experts. As stated in the findings of Shane Rappoli's analysis on organizations, he suggests that M-type organizations are able to leverage experts and ideas more effectively than matrix-type organizations.[124] This is key because SMEs, as discussed earlier, are paramount in identifying and solving the complex issues in cyberspace.

A qualitative analysis of the literature on DoD and theoretical organizational structures suggests that despite being a hierarchal and mechanistic organization, the creation of the cyber mission force teams has provided the DoD with an adaptive organizational structure that utilized its SMEs to combat cyberspace threats. Additionally, this structural design allows for easy assimilation of additional personnel to perform cyber operations.

Current Cyber Militia Employment, Cost and Effectiveness

A case study analysis on select current militia and "militia-like" organizations from around the world provided much needed information to assess the value of a cyber militia. The organizations selected provide a swath of the who, what, where, when, and why current cyber security organizations exist. This information was used to determine the varying impacts they have had in their respective countries. The groups studied are from Estonia, India, Russia, the United Kingdom, and two international groups, the Electronic Frontier Foundation and Anonymous. Each group was dissected into seven parts: State affiliation, type and size, mission, context in which it was formed, member

[124] Shane Roppoli, "Does It Matter How the US Army Organizes To Deal with Cyber Threats?" (Monograph, School of Advamced Military Studies, Fort Leavenworth, KS, 2012), 32.

compensation/cost, risk reduction measures (as applicable) and notable actions (highlighted by successes). By comparing and contrasting the characteristics of these groups, common themes have emerged and are discussed in the analysis summary.

The first group analyzed was Estonia's Cyber Defense League (CDL). Created as a direct result of a three week cyber barrage attributed to Russia and its supporters, it is one of the best examples of what a cyber militia is and how it can support a country's territory in cyberspace. The following table details key traits of Estonia's CDL.

Table 2. Estonian Cyber Defense League

Comparison of Current Cyber Organizations - Estonia				
Name (Year Formed)	**Actor**	**Type / Size**	**Purpose/Mission/Roles**	**Strategic Context**
Estonian Cyber Defense League (2011) http://www.kaitseliit.ee/en/edl	State	Hierarchy ~100-300 members	Peacetime: - The raising of society's awareness regarding cyber threats - The sharing of knowledge among IT specialists in the field of information security Crisis: - Performs missions as directed by the Defense League, dealing mostly with the protection of the cyberspace around critical infrastructure	- Nation of 1.3M people, large volunteer defense league, small economy, occupied by Sweden, Denmark, Germany, USSR, Russia - Extremely patriotic population that is cyber savvy - 2007 Cyber attacks have served as a rallying cry to defend their country
Compensation	**Risk Reduction**		**Notable Missions/Successes**	
Training / Opportunities to collaborate with experts in field	- Background Checks - Under direct control of DoD equivalent - Must follow Estonia Cyber Laws / Code of Conduct		- Acted as a ready reserve for CERT-EE during the country's parliamentary elections - Organizes and participates in strategic and tactical level exercises	

Source: Created by author with information from Kaitselitt Estonian Defense League, "The Defense League," last modified 1 January 2015, accessed 13 February 2015, http://www.kaitselitt.ee/et/kl.

Estonia's CDL is the smallest of the militia's studied. This is partly attributed to the country's comparatively small population but is also a direct result of the application process to join. They not want only highly qualified individuals (must be Estonian) but also require background checks before membership can is granted. Though no readily available quantifiable data has been uncovered showing the CDL's direct impact on cyber-attack reduction, there has not been a repeat of the 2007 events that led to its formation.

Next is India's Cyber Army (ICA), and at first glance may too seem like the classic state-sponsored militia. However, it is a non-state entity run by an entrepreneur, exhibiting more similarities to a private company than an entity organized for the common defense of a country. Initially formed to combat cyber-attacks from actors within Pakistan, the ICA is a cyber activist group that aligns itself with what it believes to be in India's best interests. It receives no funding from the Government of India and therefore runs courses that members must pay for as a way to support itself. It has coordinated with (just as any Indian resident can) with India's Department of Information's CERT to counter cyber-attacks and disseminate knowledge of vulnerabilities across their infrastructure.[125]

[125] Manu Kaushik, "Beware the Bugs," *Business Today*, 17 February 2013, accessed 7 April 2015, http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html.

Table 3. Indian Cyber Army

Comparison of Current Cyber Organizations - India				
Name (Year Formed)	**Actor**	**Type / Size**	**Purpose/Mission/Roles**	**Strategic Context**
Indian Cyber Army (2011) https://www.icalab.com/	Non-State	Hierarchy / Ad-hoc	- Primary is defense through collaboration and training. Organize conferences, workshops and brainstorming sessions for the advancement Information Security and Ethical Hacking. - Provide a forum for discussion on new changes, threats, loopholes and [solutions] to create a Cyber Safe India. - Author Information Security publications for all levels of readership - Share information and lessons learned with response teams, organizations and sites	- Created by concerned citizens in lieu of any formal cyber regulation from the Indian Government to counter numerous cyber crimes / attacks from Pakistan (and others) in early 2000's. - Founded/Run by Kislay Chaudhhary, Entrepreneur - Considered by most cyber security experts as a hacktivist group. - Assist general computing community in preventing and handling computer security incidents
Compensation	**Risk Reduction**		**Notable Missions/Successes**	
- Government Approved Cyber Security Certifications - ICA Provides training, but not for free.	- N/A: Anyone can join or set up individual chapters - Pay for Training / Certifications		Claims to have secured many National Websites Has been attributed to hacking/defacing multiple Pakistan websites	

Source: Created by author with information from "The Organization," India Cyber Army Organization Overview, accessed 12 February 2015, http://www.icalab.com.

The ICA has claimed to have secured many national websites and the literature has shown varying sources backing these statements. However, how the ICA performed these actions and whether or not they would have constituted as a proportionate response cannot be determined. Unsanctioned counter cyber-attacks were performed by ICA "offshoots" against Pakistan (the assumed aggressor) that only escalated cyber-attacks both in quantity and in complexity instead of deterring them. The ad-hoc nature of the

cyberspace actions taken by the ICA show a less structured, yet however highly motivated group (unknown size) of individuals that are loosely led by a citizen and entrepreneur. They have become a force that adversary actors must be wary of but are not the deterrent that Estonia's CDL has seemingly formed itself to be.

The third actor studied was Russia, which has an array of cyber militias and cyber mafias conducting cyber warfare in one form or another. Having blurred the line between criminal and war waging activities, Russia is exploiting outdated UN policies to push political agendas and steal approximately four billion dollars a year through cyber activities.[126] The most infamous of these groups was the "Nashi" which was initially a grass roots youth movement that took to the cyber domain to advance its global presence. Table 4 outlines some of Nashi's key characteristics and notable (infamous) actions performed in cyberspace over the past seven years.

[126] Loak Essers, "Russian Cybercriminals Earned $4.5 Billion in 2011," *Computer World*, 24 April 2012, accessed 1 February 2012, http://www.computerworld.com/article/2503653/cybercrime-hacking/russian-cybercriminals-earned--4-5-billion-in-2011.html.

Table 4. Russian Cyber Militia

Comparison of Current Cyber Organizations - Russia				
Name (Year Formed)	**Actor**	**Type / Size**	**Purpose/Mission/Roles**	**Strategic Context**
Nashi ("Ours") / aka the "Kremlin Kids" (2005-2014) Network (2014) http://www.vse-doma.su/ http://xn--e1aaooegkhc4h.xn--p1ai/	State	Forum / Hierarchy ~150,000 total, unknown amount in cyber militia sect	- End 'Anti-fatherland' sentiment across Russia. Harass Russia's Critics / Treat as Enemies of the State - Prevent foreign control of Russia - Modernization of the country and preservation of its sovereignty with that - Fight for the hearts and minds of Russia's young people in schools, on the airwaves and, if necessary, on the streets	- Nashi was formed to counter pro-Western movement in Ukraine as well as other anti-Russian groups to include neo-Nazis. Initially a "street" militia it has established itself as a technically savvy organization that utilizes computer skills across a vast range of Russian working class youth. - "Network" is the Nashi successor which keeps it pro-Russian ties but now with a tailored message for the Urban middle class.
Compensation	**Risk Reduction**		**Notable Missions/Successes**	
- Varies: Up to $1,100 dollars a month - Projects are officially funded by local business but multiple sources have cited Government officials and Nashi members acknowledging support from the Kremlin by way of monetary and verbal support. - The Group has received the equivalent of over $30M U.S. dollars from Russian State sponsored grants.	N/A: Russian uses the group through third party paramilitary forces in active defense and offensive nature. Their risk reduction measures are to simply deny involvement and punish those who speak out.		- Members of Nashi have acknowledged involvement in cyber attacks against Estonia, Georgia, Kyrgyzstan, - Online intimidation campaigns against ambassadors from the UK and Estonia - DDoS attacks against "unfriendly" newspapers - Theft of data to include videos, emails and member information from opposing groups. Some of the information was in turn used as blackmail.	

Source: Created by author using information from Wikipedia, "Russian Nashi (Youth Movement)," last modified 6 May 2015, accessed 1 June 2015, http://en.wikipedia.org/wiki/Nashi_(youth_movement)/.

The Nashi, formed as a street gang in 2006, quickly evolved as its member base grew and incorporated a technically savvy following of disgruntled Russian youth. Initially an ad-hoc group based around the forum model of operations, its size allowed it to be successful in large scale DDoS attacks against pro-Western or anti-Russian newspapers. These successes caught the attention of various Russian state officials and the Nashi quickly restructured itself into a hierarchy to perform cyber-attacks synchronized with Russian military ground attacks into Georgia. This very large, well-funded, state-sponsored cyber militia poses a serious threat to any state or non-state actor across the globe.

The United Kingdom's Warning, Advice, and Reporting Point (WARP) is more of an online neighborhood watch program than a group of cyber security individuals. A partnership between the state and these online community's exists primarily as a way to collect and share information. Data provided by the WARP is used by government security organizations and in-turn the government produces substantiated threat bulletins that the WARPs use to better protect private entities in cyberspace. Cyber security data is contributed by members (anyone in that WARP's online community), filtered, and then disseminated by an "operator" volunteer that coalesces it into pertinent information for that specific WARP. Table 5 provides an overview the WARP framework.

Table 5. United Kingdom WARP

Comparison of Current Cyber Organizations United Kingdom - WARP				
Name (Year Formed)	**Actor**	**Type / Size**	**Purpose/Mission/Roles**	**Strategic Context**
United Kingdom - Warning, Advice and Report Point (2002) https://www.warp.gov.uk https://www.warpnetwork.org/index.html	State - Public / Private Partnership	Hierarchy / Cell 10 Main WARPs, each with 2 or more sub-WARPs containing 20-100 individuals. Estimated total is ~2,000 members	- Providing a cost-effective, trusted environment where members of a community can enhance their information security by sharing problems and solutions. - The WARP operator decides what cyber-security information is relevant, delivers it to the community, facilitates the sharing of advice and best practices, and builds trust within the community, so that members report incidents to each other	The WARP program was created in 2002 by the National Infrastructure Security Coordination Centre (NISCC), now part of the Centre for Protection of National Infrastructure (CPNI), to allow WARP members to receive and share up to date cyber threat information and share best practice. WARPs are now provided by CERT-UK, becoming part of their wider strategy for supporting trusted information sharing.
Compensation	**Risk Reduction**		**Notable Missions/Successes**	
- Privileged access to cyber threat and vulnerability information and solutions in a trusted forum - Early warning of cyber threats and vulnerabilities - Ability to learn from experiences, mistakes, successes of other users and seek advice - Improved personal ability to protect a network	Activaties are monitored / audited at National level		- Successes have been mainly at the local level, facilitating better cyber security and information security practices at various cities, towns and universities. - Just recently tied into to the UK's - Cyber Emergency Response Team (CERT). Provides data points for suspicious cyber activity at local level while providing a pool of volunteers to combat/aide in the resolution of possible large scale cyber incidents.	

Source: Created by author using information from United Kingdom Warning, Advice, Reporting Point, "About Us," last modified 20 December 2014, accessed 7 February 2014, https://www.warp.gov.uk.

The key person or set of persons in the WARP structure are the volunteer "operators" who establish and run the day to day or (weekly) information dissemination

activities. These volunteers are important because they basically determine what is useful and what is not and this requires some level of expertise. Producing literature on real versus fake threats, best practices, and helpful advice, requires not just expertise but a high level of dedication. These volunteers have shown to be quite a resource, as the WARPs have provided enough useful information as to warrant inclusion into the UK's CERT program. The WARP, albeit not a standard militia, could be used to assemble one. The WARP has value in the information sharing provided to interested parties and provides a possible subset of tasks that could be performed by a similar US-based volunteer organization.

Similarly, The EFF represents an organization of concerned citizens rather than a full blown militia. However, their structure, membership experience and collaborative cyberspace efforts that drove varying successes should be applauded and studied. Founded in California in 1991, the group boasts a renowned collection of cyberspace and freedom of speech experts and activists of over 50,000 members. Details are examined in table 6.

Table 6. Electronic Frontier Foundation

Comparison of Current Cyber Organizations Electronic Frontier Foundation				
Name (Year Formed)	**Actor**	**Type / Size**	**Purpose/Mission/Roles**	**Strategic Context**
Electronic Frontier Foundation (1990) https://www.eff.org/	Privately Funded Non-Profit	Forum Cell Hierarchy 50,000 international members ~60 employees Board of Directors Advisory Board	- Defends civil liberties in the digital world - Champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development - Work to ensure that rights and freedoms are enhanced and protected as use of technology grows.	Formed in July 1990 by John Gilmore, John Perry Barlow and Mitch Kapor in response to a series of actions by law enforcement agencies that led them to conclude that the authorities were gravely uninformed about emerging forms of online communication and that there was a need for increased protection for Internet civil liberties.
Compensation	**Risk Reduction**		**Notable Missions/Successes**	
- EFFector, EFF's weekly e-newsletter - Action Center Alerts - Invitations to Members-Only Speakeasy meetups (aka networking) - Digital EFF Member badge for your site or blog - 10% discount at EFF's online store	N/A: International membership for anyone who would like to donate a minimum amount of money.		- 1990-94: Supported Steve Jackson in his legal battle against the U.S. Secret Service in which the Government was found to have wrongfully seized electronic data from Jackson and his company. - 1994: Cracked the U.S. Government's Data Encryption Standard (DES) in less than 23 hours, the final death blow for DES, resulting in its eventually replacement by the Advanced Encryption Standard in 2002. - Current software and development projects include "Switzerland", a tool that detects violations of network neutrality and "HTTPS Everywhere" which makes Firefox use secure HTTP to the greatest extent possible. - Actively campaigning against current NSA monitoring (spying) practices. - Current white paper include "Defend Innovation: How to fix our broken Patent System" and "Who has Your Back? 2014: When Copyright and Trademark Bullies Threaten Free Speech."	

Source: Created by author using information from Electronic Frontier Foundation, "About," last modified 31 May 2015, accessed 1 June 2015, https://www.eff.org/about.

Anonymous, once the epitome of a non-state cyber nuisance, has morphed into a collection of individuals that went from "trolling" the Internet to exploiting its "many to many" communication technology to advance its anti-censorship, and anti-government control beliefs. Table 7 provides a condensed overview of Anonymous.

Table 7. Anonymous

Comparison of Current Cyber Organizations Anonymous				
Name (Year Formed)	**Actor**	**Type / Size**	**Purpose/Mission/Roles**	**Strategic Context**
Anonymous (2003) http://anonofficial.com/ http://en.wikipedia.org/wiki/Anonymous_(group)	International Non-State	Forum and Cell / ~5,000 members	- Anti-Cyber Surveillance - Anti-Cyber Censorship - Internet Activism - Internet Vigilantism	- Purpose and Mission has changed since its inception. Originally a small group of hackers/cyber pranksters, the group began to take on a hacktivist role as small cells began to coordinate larger scale attacks against Scientology. -"Anons" oppose internet censorship and control, and the majority of their actions target governments, organizations, and corporations that they accuse of censorship. Anons were early supporters of the global Occupy movement and the Arab Spring. Since 2008, a frequent subject of disagreement within Anonymous is whether members should focus on pranking and entertainment or more serious (and in some cases political) activism.
Compensation	**Risk Reduction**		**Notable Missions/Successes**	
Social Affiliation	N/A: Membership is open to all		- Most recently declared war on ISIS and has harassed any online ISIS footprint they can find to include "taking down" 800 twitter accounts, 50 email accounts, 12 Facebook pages and a half dozen websites. - Earlier targets of Anonymous hacktivism included government agencies of the US, Israel, Tunisia, Uganda, and others; child pornography sites; copyright protection agencies; the Westboro Baptist Church; and corporations such as PayPal, MasterCard, Visa, and Sony. Anons have publicly supported WikiLeaks and the Occupy movement.	

Source: Created by author using information Gabriella Coleman's, *Hacker, Hoaxer, Whistleblower, Spy: The Many Face of Anonymous* (Brooklyn, NY: Verso, 2014).

Summary of Case Study Analysis

A comparison of current cyber organizations shows a variety of ways to form and utilize a volunteer force dependent upon the context of their formation. The case can be made that each was created initially as a defense mechanism to protect what each believed was a threat to a way of life. The Russian Nashi, most associated with aggressive and offensive cyberspace behavior was founded to defend against what they perceived to be an infiltration of anti-Russian influence. The Russian State capitalized on this "youth movement" and incorporated them into cyber campaigns against Estonia, Georgia, and Kyrgyzstan. In turn, they formed volunteer cyber organizations to defend against pro-Russian influence in the countries most affected by Russian aggressiveness. The creation of the Indian Cyber League was to defend against Pakistani cyber-attacks and in turn, more Pakistani groups materialized to defend against India. Each militia was fashioned by a rallying cry of sorts, a patriotic call to duty to defend or retaliate against a specific threat or sets of events. This same rallying cry is evident in the genesis of the EFF and even Anonymous. The defense of civil liberties, government transparency, and accountability are themes that weave through most of what the EFF and Anonymous do.

The context or the "why" a group was created drives its mission or purpose. A common purpose was each group's desire to share knowledge, develop awareness, and hone cyber domain expertise. They understand that they are stronger through collaboration and that numbers matter (just as in the other domains) when it comes to deterrence. As a group, each has had relative successes. Estonia has not had a major cyber incident in years and their successes have become a case study for group and

governments worldwide looking to mimic their success.[127] Even the more aggressive of the groups studied, Russia and Anonymous had to share knowledge and collaborate on "projects" or operations to ensure success.

The purpose and mission of a group drove its operational practices (defensive versus offensive) which ultimately determined the group's structure. The defensive operations of Estonia naturally formed into a hierarchal type of militia (a centralized command and control structure as outlined in chapter 2) under its current defense league structure. This is the also dominant type albeit not necessarily the only type of militia seen within the Indian, UK–WARP, and EFF organizations. These defense and knowledge sharing based groups have a general top-down structure but have been formed into large cells based on geographic location in order to facilitate the size of the organization. Estonia's militia is surprising small and is located for the most part within Estonia. The more offensive minded groups are much more loosely formed. Anonymous is the classic forum in which individuals discuss operations in large virtual chat rooms and a leader or group of leaders emerge based on desire and skill. The forum would dissipate into smaller cells (almost always down to the individual level) dependent upon the operation it was undertaking to execute attacks along different cyber-attack vectors. Interestingly, Coleman observed from her study of the group Anonymous, that once their "persona" became identifiable with an individual, a hierarchal structure would form, and that structure would always result in failed activist operations. Coleman concluded that

[127] Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis, "Estonia's Cyber Defence League: A Model for the United States?" *Studies in Conflict and Terrorism* 36, no. 9 (2013): 778-779.

almost always, "Loose coordination would maximize effects."[128] Thus, offensive cyber operations for the purposes sought by Anonymous failed unless they remained "group-think" in nature.[129] Applegate argued the opposite in his description of how a US cyber militia would operate, as he believed it would most likely be best suited to perform defensive operations.[130] The Russian Nashi exhibited similar traits to Anonymous, working in forums to recruit and gather members for coordination before breaking apart into cells to execute individual attacks. In the case of Russian cyber militias, however, there is evidence of governmental direction to perform certain actions within specific time windows. This was the case in the Georgian campaign where cyber-attacks occurred before and during the Russian ground invasion.[131]

The countries represented in the case study analysis have differing sized economies and thus their dependence on their respective cyber organization varies. The Estonian and Indian Cyber militias were stood up because the standing Government lacked the means to effectively handle the defense of their cyber border on their own. This reliance has magnified their impact. The prospect of incorporating skilled cyber individuals on an as needed basis is appealing in theory due to the potential fiscal benefits in having free "on-call" or "surge" personnel capabilities. Ultimately, however there are indirect costs for a state-sponsored militia either to ensure authorized access via a vetting

---

[128] Gabriella Coleman, *Faces of Anonymous,* Kindle Edition, 205.

[129] Ibid.

[130] Applegate, *Leveraging Cyber Militias,* 14.

[131] Shachtman, "Kremlin Kids."

process (Estonia) or to mission performance against specific targets (Russia). For example, Estonia's members provide all their technical expertise free of charge but because they require background checks there is an indirect cost in terms of paid government personnel performing their duties in effort to obtain the right individuals. The UK-WARP partnerships require private contributions and donations but has state-backed individuals at the Center for Protection of National Infrastructure (CPNI) and the British Central Volunteer Headquarters (CVHQ) to coordinate responses to incidents that require CERT initiation. The EFF and Anonymous both receive donations for continued operations and pursuit of legal objectives, while India charges for technical training and services.[132]

Finally, the mission and purpose of a group drove how they mitigated risk. State-sponsored organizations had some type of "checks and balances" system in place to mitigate unauthorized access to insider threats. Estonia's application process is the most comprehensive and it is telling that a country that prides itself on its technical prowess, despite its small economy, has such a small (some argue elite) militia supporting its regular standing military. This could also just be a factor of scale as Estonia's population is just 1.3 million people or roughly the size of San Antonio, Texas.[133]

This analysis provides examples of organizational structures, missions, and risk reduction measures that have proved to be effective and comparatively low cost for

[132] India Cyber Army Website, "Organization Overview," accessed 22 January 2015, https://www.icalab.com/.

[133] Country of Estonia Website, "Estonia at a Glance," 4 January 2015, accessed 18 January 2015, http://estonia.eu/about-estonia/country/estonia-at-a-glance.html.

possible inclusion into a volunteer US cyber organization. This section briefly described what a militia may look like and the missions it could perform by comparative analysis to current cyber militias. How to raise a militia within the constraints of the current operating environment, specifically within the US is addressed in the following section.

Raising a Militia

Raising a militia will require several lines of effort in order to overcome the legal and political constraints identified as part of the current operating environment earlier in this paper. Legally, the US Congress would be within its purview to call upon "able bodied" individuals to defend against threats in cyberspace. However, the United Nations has not updated security resolutions on a country's "right to war" in over 60 years. As such, the law of armed conflict does not specifically state what is and what is not an actionable threat in cyberspace. Civilian involvement in offensive cyber warfare will consequently be defensive, at least in part. Whether an attack targets the electrical grid, the financial system, the air traffic control system or any of a host of other infrastructure components, it will involve directing hostile traffic at the computer systems used by the target entities.[134] At that point, the computer staff of the target entities is in a position analogous to that of soldiers who are being attacked by the military forces of enemy nation-state; their position is probably most analogous to that of a harbor fortress being shelled by enemy ships. Like the soldiers in the fortress, computer personnel confronting a cyber-attack will be responsible for defending their "territory" from hostile activity;

[134] Brenner and Clarke, *Conscripts*.

their primary defensive goal will be to keep their systems functioning despite attempts to shut them down.[135]

The public debate on more cyber security has varied but if there were ever a time to propose a militia now may be it. History may view 2014 as the worst year on record for data breaches (more than 700) to include the large scale losses at Target, Jimmy Johns, Sears, and Sony, the public outcry for better security has never been louder. The high water point of American ire towards those who would attack the core value of freedom of speech came right as the year was about to end. The late November cyber-attack against Sony Pictures and the subsequent cancellation of the movie (albeit short-lived), *The Interview*, unified an American public to a higher degree hat no previous cyber-attack had. The possibility of a state actor threatening the American way of life (even calling for "9/11 equivalent" attacks on the US public) harkened a call to arms of sorts that had not been heard since the dark days following 9/11. However, this time around the demands for a cyber response replaced calls for kinetic retaliation (i.e. bombing northern Afghanistan). Sony released *The Interview* via Google+, Xbox Live and Microsoft.com and within four days, 2 million people had downloaded it.[136] Several days later, a massive unattributed DDoS attack blocked North Korean access to the internet for more than 24 hours. The attack has since been attributed to the hacktivist

[135] Ibid., 24.

[136] Eric Schwartz, "The Interview's Online Box Office Blew Theaters Out of the Water," DCInno.com, 28 December 2014, accessed 20 January 2015, http://dcinno.streetwise.com/2014/12/28/how-many-people-watched-the-interview-opening-weekend-online-crushes-box-office.

group, Anonymous, which surprised only those who had not been following their more recent activities.[137] The response was remarkably effective for having been coordinated in such a short amount of time and showcased how a loosely knit, albeit skilled organization can quickly form to take action in cyberspace. Some have speculated that the US Government was involved in some manner as well, but no direct evidence has been produced to support this claim.[138]

True or not, it was not the actions taken in cyberspace that were most important concerning the Sony incident. Rather, it was a hastening of the political response by President Obama through two executive orders and addressing the issue personally in his state of the union address on 28 January 2015. Additionally, President Obama made it a point to address expanding current cyber law and of note is the fact that hacking would now be in the category of racketeering. What this does is penalize anyone even associating with hackers and hacker groups breaking the law. Thus, current patriotic hackers and hacktivists groups will have a much tougher time in protecting networks as they will no longer be able to perform some of the cyber operations (such as penetration testing) that disrupt cyber criminals. On the other hand, Robert Graham, a cybersecurity professional and routine contributor to the Errata Security Blog, has detailed the proposed law changes by emphasizing that, "The most important innovators this law would affect

---

[137] Cecelia Kang, "North Korean Web Goes Dark After Obama Pledges Response to Sony Hack," *Washington Post*, 22 December 2014, accessed 10 April 2014, http://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.

[138] Ibid.

are the cybersecurity professionals that protect the Internet."[139] This is because he and others fear that the new laws would prohibit defenders from performing necessary cyber defense actions rather than deter offenders.

No matter what new US laws or Presidential edicts that are put in place to support cyberspace security, it will take several years for international laws to catch up. Cyberspace and the laws that will ultimately be codified to assure safe access to it are considered a study unto itself. It is possibly the most complex and perhaps the most important of the issues that need to be addressed to ensure the US's desired cyberspace end state of assured access. With these considerations in mind, the following section proposes possible organizational frameworks and operating concepts for a US government sponsored cyber militia.

Potential Framework and Operating Concept of a US Cyber Militia

The research revealed a variety of roles, responsibilities, and structures that could lead to the incorporation of a US cyber militia. A US cyber militia would more than likely need to be born out of a nationally recognized professional association of cyber security professionals and enthusiasts. Unfortunately, at this time, there is no single US entity that fills this role.[140] The Information Security Systems Association (ISSA), EFF, and US-CERT provide talent pools (among others), offer possible organizational

[139] Robert Graham, "President Obama is Waging a War on Hackers," *Wired*, 15 January 2015, accessed 3 February 2015, http://www.wired.com/2015/01/president-obama-waging-war-hackers.

[140] Spidalieri and Kern, *Professionalizing Cybersecurity*, 1-2.

structure and mission sets that could form the basis for such an organization. Air Force Lieutenant Colonel Sean Kern recommended such as organization in his study concerning the professionalization of the cyber workforce. Kern argued that a national professional cyber association is needed to address the shortage of qualified cyber security personnel, "[it would] solidify the field as a profession, support individuals engaged in [the] profession, establish professional standards…and support the public good."[141] The key for this national organization would be to make it open to US citizens only with a corresponding mission set that promotes national cyber defense. Achieving cybersecurity, in other words, is far more than a technical problem: it is fundamentally a people problem.[142]

Garnering the necessary volunteers is just the first step however, as an organizational model and concept of operations will ultimately need to be in place (and modifiable) to structure efficient operations. The first analogous framework would be that of a volunteer fire department. This is a great comparison as there seems to be no end in sight for "cyber fires," and "local" cyber fire fighters would theoretically be able to respond more quickly to an incident if it occurred in their space. On call "24/7", a volunteer cyber department would have a similar concept of operations. "Cyberteers" would be "on alert" waiting for an alarm and once it sounded they would be able to quickly perform the necessary DCO in response to an incident. This is no different than what is being down now across DoD except that this model frees up professional

[141] Ibid., 2.

[142] Ibid., 4.

combatants to pursue the more aggressive active response measures prescribed for long-term deterrence. Additionally, fire departments routinely perform preventative operations known as outreach programs that aim to diminish fires at the source such as carelessness around flammable materials. Cyber department volunteers would act in a similar manner as well, providing expertise and training to improve on the basic things required to prevent successful cyber-attacks. Lieutenant General Edward Cardon, Army Cyber Commander, emphasized three things in a speech on Army Cyber to majors at the General Command and Staff College. Using research from FireEye, a network and software security company, he identified that, "80 percent of all cyber-attacks can be prevented network architectures, patching frequencies and end user operational security practices."[143] A group of volunteers that focused on an organization's performance in these three areas would not only hone end user cyber security but would free up full-time personnel to perform those active defense measures to prosecute and attribute threats "further out" in cyberspace.

Another analogous organizational model is the Civil Air Patrol (CAP). The government created CAP in 1941 after more than 150,000 aviation enthusiasts convinced it to incorporate them formally into an organization in which they could serve their country in some capacity while doing what they loved. The CAP has an amazing history of support in civil air operations (to include German U-boat chasing along the coasts in WWII) and continues to serve today by performing 90 percent of all inland search and

[143] Cardon.

rescue missions.[144] Commanded by a Two-Star General and formally headquartered out of Maxwell Air Force Base, the CAP organizational construct and mission statement could easily be molded into a "Civil Cyber Patrol (CCP)." In fact, there are seeds in place that could support rapid growth of such an organization. The CAP, understanding the changing operating environment has channeled its tech savvy members into the Air Force Association's CyberPatriot competition for the last seven years. CyberPatriot is an annual competition held by the AFA's National Cyber Education Program that pits teams from all over the country against each other in a virtual network environment representative of today's large companies.[145] Competitors work as a team to discover vulnerabilities and deflect cyber-attacks with the winners ultimately ending up in Washington, DC to be honored.[146] A volunteer organization could fall under the command of either the active or reserve cyber components of each service (reference figure 2), fulfilling missions dictated by the units they are assigned to.

Answering the Primary Research Question

Could a US cyber militia as constructed in this study be an efficient and cost effective organizational augmentation in support of DoD cyber operations? The short answer is yes, but it would take some time to realize the potential benefits of a cyber militia. The amount of time could possibly dictate implementation because if it takes too

---

[144] Civil Air Patrol, "A History of the Civil Air Patrol," 11 June 2014, accessed 27 March 2015, www.gocivilairpatrol.com/index.cfm.

[145] US CyberPatriot, "What is CyberPatriot?", 12 September 2014, accessed 27 March 2015, http://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx.

[146] Ibid.

long, the gaps discussed earlier in this paper may have been filled through another means. The original idea of the cyber militia was that it would be a short-term fix to plug those gaps. There would be a slight impact in the short term if the government created cyber volunteer defense organization and effectively offloaded one or two mission sets. Much in the same manner that the CAP worked shore defense and inland rescue missions of downed aircraft, the CCP would need a mission set they could harness their energies on and be the subject matter expert for a specific threat or activity. CCP enduring impacts too would most likely follow the CAP, as their activities over the decades helped decrease civil aviation accidents and promoted safer flying standards.[147] A CCP that focused on proliferating information leak prevention and safe cyber practices in conjunction with several of the other national/international recognized cyber associations could have a long-term impact on reducing the root of cyber incidents: bad personal security.

At the heart of the cost efficiency question is what in reality can a volunteer force provide a regular standing professional force? What can they do with volunteer labor, many of whom would be subject matter experts in the field? The common theme from discussions with current cyber operators is penetration testing or "pentests," red teaming activities, and training. Pentests for example can be time consuming despite software automation tools due to the amount of the analysis required to set up the tests and interpret the results. This time consuming activity means it is not done as often as it should be and takes operators away from looking out beyond the DoDIN's defenses. A

[147] Civil Air Patrol, "A History."

team of volunteers could theoretically save a unit thousands of man hours each year while increasing network defenses and this savings propagated amongst the entire US cyber force quickly turns into millions of dollars. This is substantial but in the grand scheme of things a million dollar figure barely registers a percentage point when calculated into the DoD's 5.5 billion dollar cyber security budget. Thus, the cost savings impact would not necessarily be a game changer.

Increased network defenses would be by all accounts a benefit of a volunteer cyber force. However, this is difficult to substantiate as there is very little quantifiable data readily available for comparison. How many additional personnel equates to increased network defenses? The only unit of measure currently available is the number of "attacks" and those continue to increase despite more personnel, funding and technology upgrades. There is little concrete evidence to suggest that a cyber militia would drastically influence US cyber operations, especially in the short term, or the defined amount of time to "plug" the gaps or issues described in the assumption section of this paper.

The impact of a militia would most likely be a long-term return on investment. A volunteer force would include more abstract impacts in terms of partnership building, stimulating interest and honing expertise. The goal then of a US cyber militia may be to garner not only interest in a rapidly expanding and important career field but to also utilize it as a way to bridge that one percent gap between those who serve and those who do not. Unfortunately, humans can be and have been manipulated as well to forcefully or willingly divulge information that bypasses network security measures by simply circumventing them through a hard point connection. The insider threat will always be

present and it must be a consideration when and if a volunteer cyber defense force is stood up. More personnel with access to the network invariably increases the amount of possible entry ports for exploitation. Humans are the target of an equally astounding array of phishing and social engineering platforms that ultimately need to only work just once.

Analysis Summary

The analysis shows an increasing worldwide trend to augment traditional military forces with some form of enabling volunteer force mechanism. These volunteer forces have provided enough of an impact in terms of cost savings, information sharing and technical training to initiate a cyber professional "arms race" as experts in this field become increasingly hard to find or to afford. Volunteer forces alleviate resource constraints by recruiting patriotically motivated individuals willing to donate their expertise in the defense of a country's virtual cyber domain territory. The following chapter concludes this study by summarizing the findings and offering several recommendations for future researchers and decision makers to explore.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> Given that this skill set in the kind of colloquial wisdom doesn't look like a, you know, clean-cut, short-haired, wearing, you know, a white Navy uniform kind of person, how do you fold in the kind of - or find the folks with the mind set to be able to do these kinds of specific technical things and also have the mind set to be a good sailor as an example, or soldier?
>
> — Rep. Michael Conway, HIC Cybersecurity Hearing Testimony, 2014

This study briefly explored the cyber security issues currently facing the US and offered a unique solution by proposing the possibility of a volunteer cyber defense force. Capitalizing on the vast amount of cyber threat literature and the documented accounts of the actions performed by current volunteer cyber organizations from across the globe, this study has assessed that a US cyber militia could positively impact the long-term posture of US cyber defenses. The following findings and recommendations summarize the analysis performed in chapter 4.

Findings

Finding 1: The research has found that there is a substantial threat to the DoD and US national security via the cyber domain as cyber-attacks have increased in quantity and complexity over the past five years. There are numerous actors with a large array of easily accessible tools that poise varying degrees of risk to DoD command and control automated information and weapon systems.

Finding 2: Despite the estimated worldwide deficit of cybersecurity professionals estimated to be somewhere between 500,000 and 1 million,[148] the US has in place the people, organizations, systems, and processes to stand-up a large volunteer cyber force. With universities producing an estimated 20,000 cyber security professionals a year and another 900 PhDs, all with the technical skills to perform cyberspace operations, the US talent pool is quite large and growing.[149] Although there is no national level cyber professional organization, there are an abundance of groups ranging in forms across the US that could easily be integrated into some form of collaboration and sharing network. Additionally, there is an array of free tools, training and online collaboration forums available to anyone interested in honing their cyber security expertise. For example, DISA's Federal Virtual Training Environment (FedVTE) teaches individuals how to monitor a network, perform basic pentests and provides the computer tools necessary to enhance ones technical skill in the cyber domain. DHS also now has a free Cyber Core Academy open to anyone in the DoD and the National Defense University offers a free Master of Science in Cyber Security to active duty personnel.

The large amount of current organizations, informal cyber security groups and training opportunities available in the US is a valuable resource that has yet to be fully

[148] Violet Blue, "Cybersecurity's Hiring Crisis: A Troubling Trajectory," ZDnet 25 August 2015, accessed 28 April 2015, http://www.zdnet.com/article/cybersecuritys-hiring-crisis-a-troubling-trajectory.

[149] Martin C. Libicki, David Sentry, and Julia Pollack, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (Washington, DC: Rand Corporation, June 2014).

tapped. Formalizing the career field, and standardizing terms, duty titles, and certifications would go a long way in harnessing US cyber resources.

Finding 3: A supplemental all-volunteer force would need to start small, initially be formed near Cyber Command or one of the service cyber headquarters, and it would be best-suited legally performing defensive operations under DoD's current hierarchal organizational structure. Starting small and near a location with current DoD Cyber professionals allows for more consistent face-to-face interaction which would facilitate a smoother initiation and ramp-up of capabilities. Having volunteers work with DoD near or in their hometown should cultivate a mutual trust to grow more quickly between the regular and volunteer forces. Understanding that one of the benefits of the cyber arena is the fact that it bridges vast physical distances. However, this risk reduction measure would ease security concerns from decision makers and facilitate the quick victories needed to confirm a militia's viability. One of the immediate benefits of a volunteer cyber force is the freeing up of regular forces to focus further out in the DoDIN defense layers.[150]

Finding 4: Non-state and criminal actors are most likely only deterred through military retribution, be it kinetic or cyber related. In fact, Franklin Kramer argues against the military based approach all together as he believes state actors would most likely be susceptible to soft power responses from diplomatic, economic or even informational forms of punishment.[151] In other words, additional defense is not going to reduce the

[150] Applegate, *Leveraging Cyber Militias*, 17.

[151] Kramer, *Cyberpower and National Security*, 15.

amount of cyber-attacks on the US. A cyber militia may strengthen defenses and bring critical expertise in times of crisis but it would not be able to perform the missions that would effectively reduce attacks at the far left end of the kill chain. This more offensive or proactive defensive mission is something a cyber militia could do, but is most likely not something the US would implement for political reasons.

Finding 5: A cyber militia could be used in a training role to hone active and reserve component personnel. Specifically, they could be utilized in keeping the 2,000 reserve component members up to date on current cyber security best practices as well as new techniques to incorporate into operations.

Finding 6: Cyber volunteers would most likely need some form of legal protection. State and non-state actors will target cyber militia personnel as a means of defense but other threats, such as the "trolls" of the internet, are also a danger. The current generation of tricksters would enjoy nothing more than to impede cyber operations that violate their personal moral code. They would do it to prove perhaps a minor point that aligns with their beliefs ("sticking it" to big Government) but more than anything they would do it for the "lulz" or their version of humor.[152]

Finding 7: Last but just as important is the finding that whatever form a volunteer workforce takes, it should most likely not be called a militia. Words matter and the term militia does not immediately invoke the type of team the DoD would want to control nor what the general cyber security professional may want to join. Calling it a militia would most likely kill the volunteer force idea before it could get the chance to prove itself as a

[152] Coleman, *Many Faces of Anonymous*,101.

viable option. Current militia-like forces are called Cyber Defense League or People's Cyber Army. A more recent non-cyber militia were the 100,000 Iraqi Sunni's called the Sons of Iraq that were stood up as a "home guard" to fill the security gaps in the Iraqi security forces.[153] Be it a US Cyber Guard, Civil Cyber Patrol or Cyber Defense Legion, a cyber volunteer force will require a name and a definition that is publically and politically acceptable for federal incorporation.

Recommendations

Recommendation #1: A comprehensive study of the United States population and their desire to volunteer in a military cyber defense program. The topic of a possible US cyber militia should be proposed to the DSB or Air Force Science Advisory Board (AFSAB) for a "deep-dive" into topics briefly discussed in this study. A DSB or AFSAB led study would provide experienced researchers from academia, industrial and the US government the required access to thoroughly assess the viability of a US cyber militia. Data should be gathered from varying regions, companies, universities and professional associations to assess interest and determine compensation/reward if needed. Understanding the breadth and depth of volunteers is important before any trial program becomes operational. This proposed study should be able to gauge the amount of time a volunteer would be willing to donate in a given week and determine a threshold level for what some may deem as an "intrusive" background check as well as any other necessary application requirements such as determining skillset.

[153] Mark Wilbanks and Efraim Karsh, "How the Sons of Iraq Stabilized Iraq," *Middle East Quarterly* (Fall 2010): 57-70, accessed 4 April 2015, http://www.meforum.org/2788/ sons-of-iraq.

Recommendation #2: The study showed a hierarchal militia structure would be best suited for incorporation into active service component organizations. This would allow for the vetting of possible members and the utilization of control measures required for acceptable risk mitigation. However, this should not preclude investigating the possibility of forming the militia under the control of DHS. With a similar organizational structure and funding line, the DHS mission could arguably warrant a militia's incorporation just as much as the DoD.

Recommendation #3: A team of current US cyber operations military personnel at USCYBERCOM with representation from each service and component should be formed to discuss and assess the viability of a US cyber militia. Having a plan of how to incorporate a civil volunteer workforce into current cyber operations would frame the feasibility of such a concept while initiating a contingency plan that could ultimately be used to manage a cyber crisis.

Recommendation #4: The study suggests that a hierarchal militia model is best suited for defensive operations. Thus, volunteer activities should be defensive in nature. This reduces the risk of breaking any laws and keeps volunteer user access to a specific layer of defense. A framework similar to that of the CAP be used to create a volunteer cyber organization of Civil Cyber Patrol (CCP). The creation of two initial CCP elements should be studied in further detail. The first element should be established in the vicinity of the greater Baltimore/Annapolis Maryland area and fall under the control of the 175th Network Warfare unit. Their work with the Estonia CDL would leverage any lessons learned/best practices that materialized from several years of interaction. The proximity of US Cyber Command headquarters at Fort Meade as well as to the DC area would

provide many opportunities of face-to-face interaction between controlling elements and a large array of technology based companies and universities with qualified pools of possible volunteers. Again, face-to-face interaction is key in gaining that mutual trust required for early and long-term success. The second recommended area to initiate a volunteer cyber force would be in San Antonio, Texas. Home of the 24th Air Force as well as the Cryptologic and Cyber Systems Division (containing the subordinate PKI program office…aka birthplace of the Common Access Card), San Antonio has a large, military friendly population locals refer to as "Military City USA." More intriguing would be the response from neighboring Austin, just 60 miles north. Many consider Austin as the silicon valley of Texas. It has a large contingent of some of the most well-known US tech companies that include Microsoft, Google, and Dell. The local ISSA chapter is extremely large and has won several awards the previous four years.[154] Along with its numerous colleges and universities, Austin would provide some insight into how a city that is better known for "staying weird" than its support of the military or Government would respond to a call for military volunteerism. Austin would be an ideal candidate to increase civilian-military interaction as a way to decrease that divide. This is similar to the unique, yet fruitful relationship held between the Army's Command and General Staff College with U.C. Berkley.[155]

---

[154] Information Security Systems Association Website, "Chapter Awards," 11 June 2014, accessed 3 February 2015, https://www.issa.org.

[155] Ori Braufman, "Spiders and Starfish" (Lecture, Advanced Operations Course, Command and General Staff College, Fort Leavenworth, KS, 9 December 2015).

Further Research

As identified in the literature review there are two critical information requirements that need attention prior to a decision on forming a cyber militia. The first is a study that would gauge public interest in joining a cyber militia as defined in this study. A survey of various cyber security and technology-based companies, as well as the various professional associations should be conducted to garner the range of interest on volunteering. Companies surveyed should vary in size (Google to GoDaddy) and in industry sector (technical to medical). Cyber security experts at these companies should be polled on why they might volunteer, the hours they would commit to such an endeavor, the length of service, and possible recognition (if any). Additionally, what is lacking is the DoD cyber force perspective on the use of a militia, both at the leadership and operator levels. Information from current cyber force members would be important in understanding possible "left/right" limits in collaboration efforts. This information would also hone possible mission and skill sets of possible volunteers. While at CGSC, the author engaged in unofficial discussions with a small sampling of cyber operators from every service and the reaction to a militia-like organization was generally positive. The issues in the cyber realm have been and will continue to be a very relevant topic for the foreseeable future. The importance of which warrants continued research into every aspect of the cyber domain to uncover the unique solutions required to its complex problems.

Summary

This study explored the practicality of a volunteer cyber force within the evolving cyberspace operational environment and current organizational structure of the DoD.

This organization could be mirrored after a volunteer fire department, or the Air Force's Civil Air Patrol and in all likelihood should not be called a militia. Using historical evidence as far back at the 17th century as well as case study examples from the past few years, a qualitative assessment was performed to better understand how and why militias are incorporated into active component forces. The analysis suggested that cyber militias have been useful in countries lacking the resources required to wage war with regular forces. The US government, having a dearth in one of the key resources required in cyber warfare, could find utility by expanding its recruiting pool by tapping into a pool of willing cyber volunteers. Maintaining dominance in cyberspace is paramount to maintaining long-held advantages in the other four domains and this dominance is predicated on harnessing the resource most important in its success: cyber experts. These experts have proven to be the most critical tool in the cyberspace fight and finding ways to acquire more of them should be at the top of the DoD's priority list.

BIBLIOGRAPHY

Alexander, B. Keith. “Warfighting in Cyberspace.” *Joint Force Quarterly*, no. 46 (July 2007): 58-61.

Applegate, Scott. *Leveraging Cyber Militias as a Force Multiplier in Cyber*. Fairfax, VA: Strategic Studies Institute, 2012.

Ashford, Warwick. “Powerful Cyber-Attack Tools Widely Available.” *Computer Weekly*, 3 September 2012. Accessed 2 April 2015. http://www.computerweekly.com/news/2240162578/Powerful-cyber-attack-tools-widely-available-say-researchers

Atherley-Jones, Llewellyn. *Commerce in War*. Los Angeles, CA: Methuen and Co, 1907.

Axelrod, Robert, and Michael D. Cohen. *Harnessing Complexity: Organizational Implications of a Scientific Frontier*. New York, NY: Free Press, 2001.

Becker, Corrie. “The Tallin Manual: The Legal Aspects of Cyber Warfare.” *Cyber Security and Research Institute*, 15 October 2013. Accessed 20 April 2015. http://www.cspri.seas.gwu.edu/blog/2014/7/25/the-tallinn-manual-legal-aspects-of-cyber-warfare.

Blunden, Bill, and Violet Cheung. *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware Industrial Complex*. Chicago, IL: Trine Day, 2014. Kindle Edition.

Brenner, Susan W., and Leo L. Clarke. *Civilians in Cyberwarfare: Conscripts.: an Article From: Vanderbilt Journal of Transnational Law*. Nashville, TN: Vanderbilt University, School of Law, 2010.

Cardash, Sharon L., Frank J. Cilluffo, and Rain Ottis. “Estonia's Cyber Defence League: A Model for the United States?” *Studies in Conflict and Terrorism* 36, no. 9 (2013) 778-779.

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It.* New York, NY: HarperCollins, 2010. Kindle Edition.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Face of Anonymous*. Brooklyn, NY: Verso, 2014. Kindle Edition.

Council, National Security. *National Security Strategy (March 2015)*. Washington, DC: White House Praetorian-Press, 2015.

Czosseck, C., and K. Geers. *Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam, NLD: IOS Press, 2009.

Davis, Clifford. “Army Says Only 30% of Americans Could Join.” *The Florida Times-Union,* 24 October 2014. Accessed 2 April 2015. http://www.military.com/daily-news/2014/10/24/army-says-only-30-percent-of-americans-could-join.html.

Defense Science Board. *Resilient Cyber Systems and the Advanced Cyber Threat*. Washington, DC: Department of Defense, January 2013.

Department of Defense. *Cyber Mission Analysis*. Arlington, VA: Department of Defense, August 2014.

Department of the Army. Field Manual (FM) 3-38, *Cyber Electromagnetic Activities*. Washington DC: CreateSpace Independent Publishing Platform, 2014.

Electronic Frontier Foundation. “About.” Last modified 31 May 2015. Accessed 1 June 2015. https://www.eff.org/about.

Ericson II, Clifton A. *Concise Encyclopedia of System Safety: Definition of Terms and Concepts*. Hoboken, NJ: John Wiley and Sons, 2011.

Ernst, David. “Army Fitness Standards for Fat Cyber Warriors May Change as Waistlines Grow.” *Washington Times,* 28 October 2014. Accessed 22 February 2014. http://www.washingtontimes.com/news/2014/oct/28/army-fitness-standards-for-fat-cyber-warriors-may.

Essers, Loak. “Russian Cybercriminals Earned $4.5 Billion in 2011.” *Computer World,* 24 April 2012. Accessed 1 February 2012. http://www.computerworld.com/article/2503653/cybercrime-hacking/russian-cybercriminals-earned--4-5-billion-in-2011.html.

Ferdinando, Lisa. “Dempsey: Cyber Vulnerabilities Threaten National Security.” *DoD News,* 21 January 2015. Accessed 13 February 2015. http://www.defense.gov/news/newsarticle.aspx?id=128001.

Fryor-Briggs, Zachary. “US Goes on Cyber Offensive.” *Defense News,* 24 March 2012. Accessed 2 November 2014. http://www.defensenews.com/article/20120324/EFREG02/303240001.

Geneva Convention, Relative to the Treatment of Prisoners of War, 12 August 1949, 6 UST. 3316, T.I.A.S. 3364, 75 U.N.T.S. 135.

Graham, Robert. “President Obama is Waging a War on Hackers.” *Wired,* 15 January 2015. Accessed 3 February 2015. http://www.wired.com/2015/01/president-obama-waging-war-hackers.

Greis, Justin. “The Twelve Principles of Cybersecurity Warfare.” *Art of Advice,* 6 February 2015. Accessed 19 April 2015. http://www.theartofadvice.com/2015/02/06/the-twelve-principles-of-cybersecurity-warfare.

Grimes, Robert A. “In his own words: Confessions of a cyber warrior.” *InfoWorld*, 9 July 2013. Accessed 2 April 2015. http://www.infoworld.com/article/2611471/security/in-his-own-words--confessions-of-a-cyber-warrior.html.

Harding, Joel. “Thoughts on a US Cyber Militias.” *InfoSec Island*, 23 August 2012. Accessed 1 October 2014. http://www.infosecisland.com/blogview/22224-Thoughts-On-a-US-Cyber-Militia.html.

Jarvis, Lee. *Center of Excellence Defence against Terrorism*: *Responses to Cyber Terrorism.* Amsterdam, NLD: IOS Press, 2008. ProQuest ebrary. Accessed 1 November 2014. http://www.tandfonline.com/doi/abs/10.1080/1057610X.2014.853603#. U2AZtfldXDs.

Johnson, Jay. “If 2014 Was The Year Of The Data Breach, Brace For More.” *Forbes*, 2 January 2015. Accessed 2 February 2015. http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more.

Joint Chiefs of Staff. Joint Publication 3-12 (R) *Cyberspace Operations.* Washington DC: CreateSpace Independent Publishing Platform, 2013.

Kaitselitt. “The Defense League.” Kaitselitt Estonian Defense League. Last modified 1 January 2015. Accessed 13 February 2015. http://www.kaitselitt.ee/et/kl.

Kang, Cecelia. “North Korean Web Goes Dark After Obama Pledges Response to Sony Hack.” *Washington Post*, 22 December 2014. Accessed 10 April 2014. http://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.

Kaushik, Manu. “Beware the Bugs.” *Business Today*, 17 February 2013. Accessed 7 April 2015. http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html.

Kim, Farrah. “Private Sector Spending Accelerating.” *Telecom Reseller*, 28 February 2015. Accessed 1 April 2015. http://telecomreseller.com/2015/02/28/tia-cybersecurity-report-private-sector-spending-accelerates-after-years-of-underinvestment.

Korns, Stephen W., and Joshua E. Kastenberg. “Georgia's Cyber Left Hook.” *Parameters* 38, no. 4 (August 2009) 60-76. Accessed 19 September 2015. http://search.proquest.com /docview/198032208?accountid=28992.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: Center for Technology and National Security Policy, 2009.

Lemos, Robert. “Pentagon Recruiting Drive Targets Fivefold Increase in Cyber Command.” *Eweek*, 30 January 2013. Accessed 10 February 2015. http://www.eweek.com/security/pentagon-recruiting-drive-targets-fivefold-increase-in-cyber-command#sthash.HEqQH63L.dpuf.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. New Delhi, India: Ketja, 1999. Kindle Edition.

Libicki, Martin C. *Project Air Force (US) Cyberdeterrence and Cyberwar*. Santa Monica, CA: Rand, 2009.

Losey, Stephen. “Budget to Add 4,000 More Jobs.” *Air Force Times*, 2 February 2015. Accessed 8 April 2015. http://www.airforcetimes.com/story/military/careers/air-force/2015/02/02/budget-would-add-4000-active-duty-airmen-in-2016/22740199.

MacDermott, Siobhan, and J. R. Smith. *Cybermilitia: a Citizen Strategy to Fight, Win, and End War in Cyberspace*. Birmingham, MI: IT-Harvest Press, 2013. Kindle Edition.

Marvel, Elisabette M. *China's Cyberwarfare Capability*. Hauppauge, NY: Nova Science Publishers, 2010.

McFedries, Paul. *The Complete Idiot's Guide to Weird Word Origins.* Indianapolis, IN: Alpha Books, 2008.

Mihevic, Jake. “Cyber Militias in the US: Feasibility, Structure, and Purpose.” *InfoSec Island*, 21 August 2012. Accessed 2 October 2014. http://www.infosecisland.com /blogview /22164-Cyber-Militias-in-the-US-Feasibility-Structure-and-Purpose.html.

Miller, Jennifer L. “Conducting Business in a Fast-Paced World: The Importance of Change Management.” *Student Pulse* 2, no. 10 (2010) 21-24.

Millett, Allan Reed, Peter Maslowski, and William B. Feis. *For the Common Defense: A Military History of the United States from 1607 to 2012*. 3rd ed. New York: Free Press, 2012. Kindle Edition.

Mitchell, Troy Edward. “Cyber Militias.” *Marine Corps Gazette* 98, no. 6 (June 2014): 69-72. Accessed 27 September 2014. http://search.proquest.com/docview/ 1534474230?accountid=28992.

———. “Cyber Warfare.” *Marine Corps Gazette* 98, no. 2 (February 2014): 44-7. Accessed 27 September 2014. http://search.proquest.com/docview/ 1498449009?accountid=28992.

Nakashima, Ellen. “Cybersecurity Plan to Involve NSA, Telecoms.” *Washington Post*, 2 July 2009. Accessed 19 April 2015. http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771_pf.html.

Ottis, Rain. “Proactive Defense Tactics Against Online Cyber Militia.” *Academic Conferences International Limited*, July 2010. Accessed 21 September 2014. http://search.proquest.com/docview/869507133?accountid=28992.

———. “Theoretical Offensive Cyber Militia Models.” *Academic Conferences International Limited*, March 2011. Accessed 21 September 2014. http://search.proquest.com/docview/1011054706?accountid=28992.

Otto, Greg. “4 Charts That Will Keep Federal CIOs Up at Night.” *Fedscoop*, 23 January 2015. Accessed 27 March 2015. http://fedscoop.com/4-charts-that-will-keep-federal-cios-up-at-night.

Pellerin, Cheryl. “Cyber Chief Details Cyber Threats.” *DoD News*, 2 December 2014. Accessed 9 February 2014. http://science.dodlive.mil/2014/12/02/cybercom-chief-details-u-s-cyber-threats.

Purnell, Newly. “Cyberdefense Spending Rises Amid High-Profile Hacks.” *Wall Street Journal*, 8 April 2015. Accessed 19 April 2015. http://www.wsj.com/articles/cyberdefense-spending-rises-amid-high-profile-hacks-1428487519.

Rappoli, Shane. “Does It Matter How the US Army Organizes To Deal with Cyber Threats?” Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2013.

Robert, Jordan, and Michael Riley. “Mysterious ’08 Pipeline Blast Opened New Cyberwar.” *Bloomberg*, 10 December 2014. Accessed 11 April 2015. http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

Rogers, Michael. “Cybersecurity Threats: The Way Forward.” Testimony Before House Intelligence Committee. Washington, DC: Congress, 20 November 2014.

Rosenzweig, Paul. *Cyber Warfare*. Santa Barbera, CA: Praeger, 2013.

Schwartz, Eric. “The ‘Interview’s Online Box Office Blew Theatres Out of the Water.” *DCInno*, 28 December 14. Accessed 20 January 2014. http://dcinno.streetwise.com/2014/12/28/how-many-people-watched-the-interview-opening-weekend-online-crushes-box-office.

Seul, Tim. “Militia Minds: Inside America's Contemporary Militia Movement.” Purdue University, 1 June 2012. Accessed 11 December 2014. http://docs.lib.purdue.edu/dissertations/AAI9808519.

Shachtman, Noel. “Kremlin Kids: We Launched the Estonian Cyber War.” *Wired*, 11 March 2009. Accessed 14 January 2015. http://www.wired.com/2009/03/pro-kremlin-gro.

Shalal, Andrea, and Alina Selyukh. “Obama Seeks $14 Billion to Improve Cyber Defense.” *Reuters,* 2 February 2015. Accessed 27 March 2015. http://www.huffington post.com /2015/02/02/obama-cybersecurity-defenses_n_6595620.html.

Sheppard, Donald W. “Cyber-Guard.” *National Guard* 51, no. 4 (April 1997): 36-7. Accessed 20 September 2014. http://search.proquest.com/docview/231895457?accountid=28992.

Singer, Peter W. “The War of Zeros and Ones.” *Popular Science*, September 2014, 46.

Spidalieri, Francesca, and Sean Kern. *Professionalizing Cybersecurity: A path to Universal Standards and Status*. Newport, RI: Salve Regina’s Pell Center, August 2014.

Stewart, Joshua. “Navy wants 1,000 more cyber warriors.” *Navy Times,* 23 April 2013. Accessed 22 January 2015. http://archive.navytimes.com/article/20130423/NEWS/304230016/Navy-wants-1-000-more-cyber-warriors.

Tomanelli, Steven. *Federal Acquisition Regulation Desk Reference, 15-1*. Arlington, VA: LegalWorks, 2014.

Torruella, Ramberto. “Determining Hostile Intent in Cyberspace.” *Joint Forces Quarterly* 75 (4th Qtr 2014): 114-21.

UK WARP. “About Us.” United Kingdom Warning, Advice, Reporting Point. Last modified 20 December 2014. Accessed 7 February 2014. https://www.warp.gov.uk.

US Congress. Senate. Department of Defense Appropriations Acts. S. Res. 1590. 113th Cong., 1st sess. (July 13, 2013).

———. Department of Defense Appropriations Acts. S. Res. 4870. 113th Cong., 2d sess. (July 17, 2014).

US Department of Treasury, “Remarks of Secretary Jacob J. Lew at the 2014 Delivering Alpha Conference Hosted by CNBC and Institutional Investor.” Department of Treasury, 16 July 2014. Accessed 16 April 2014. http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx.

Wikipedia. “Russian Nashi (Youth Movement).” Last modified 6 May 2015. Accessed 1 June 2015. http://en.wikipedia.org/wiki/Nashi_(youth_movement)/.

Wilbanks, Mark, and Efraim Karsh. “How the Sons of Iraq Stabilized Iraq.” *Middle East Quarterly* (Fall 2010). Accessed 4 April 2015. http://www.meforum.org/2788/sons-of-iraq.

Williams, Brett. “Cyberspace: What is it, Where is it and Who Cares?” *Armed Forces Journal*, 13 March 2014. Accessed 25 March 2015. http://www.armedforces journal.com /cyberspace-what-is-it-where-is-it-and-who-cares.

Wilshusen, Gregory, C. *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities. No. GAO-11-75.* Washington, DC: Government Accounting Office, 2011.

Zetter, Kim. “Tone Down the Cyberwarfare Rhetoric, Expert Urges Congress.” *Wired*, 3 March 2013. Accessed 3 April 2015. http://www.wired.com/threatlevel/2013/03/tone-downcyberwar-rhetoric.